AN ANALYSIS OF THE COMPUTER AND NETWORK ATTACK TAXONOMY

THESIS

Richard C. Daigle, Captain, USAF

AFIT/GIR/ENV/01M-04

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GIR/ENV/01M-04

AN ANALYSIS OF THE COMPUTER AND NETWORK ATTACK TAXONOMY

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Richard C. Daigle, B.S.

Captain, USAF

March 2001

AN ANALYSIS OF THE COMPUTER AND NETWORK ATTACK TAXONOMY

Richard C. Daigle, B.S.
Captain, USAF

Approved:

_____   _____
Alan R. Heminger (Chairman)   8 Mar 01
                                          date

_____   _____
David P. Biros (Member)   8 Mar 01
                                          date

_____   _____
Gregg H. Gunsch (Member)   8 Mar 01
                                          date

Acknowledgments

I would like to express my deepest appreciation for my wife and children for being supportive parts of this team. My wife, for always being there to take me out of the AFIT cloud, and putting my feet back on the ground by saying, take a break already. My son, for allowing me to be his role model and showing him that yes, there is a reason he's learning all that 8th grade English, Math, and Science. My daughter, for reminding me that there are more important things in life, like searching for my school work under all her Barbie toys. Thank you once again.

I would also like to express my appreciation for my advisor. His subtle, yet purposeful guidance and confidence helped me maintain my focus and drive throughout this process. In addition, his thoughtful conversations during our meetings always made for a deserved relaxing time. I can't leave out my classmates, whose support and daily company was very refreshing. Finally, I would like to thank the Cleavers, Wally and Beaver, the Taylors, Andy and Opie, and the Sanfords, Fred and Lamont, for providing much needed late night relief while working on this thesis.

Richard C. Daigle

Table of Contents

List of Figures

List of Tables

AFIT/GIR/ENV/01M-04

Abstract

The Air Force's dependence on the Internet continues to increase daily. The Internet has become a staple of the office environment along side the telephone, the fax machine, and the computer. However, this increased dependence comes with risks. The popularity and potential of the Internet attracts users with illegal as well as legal intentions. Since the Air Force considers the Internet an integral component of its Information Operations strategy, the Air Force must be confident that it can trust the security of this component. Therefore, reliable methods and information that helps the Air Force classify the risks associated with the Internet can help the Air Force determine the best processes to assure the security of its use of this resource.

This thesis examines the computer and network attack taxonomies developed by John Howard. Howard developed the taxonomy to help him classify Internet security incidents as part of his doctoral research and as part of a follow-on project to develop a common language for computer security. The taxonomy is a possible method that the Air Force can use to help it classify Internet security attacks and incidents.

This researcher concluded that the computer and network attack taxonomies were satisfactory. The questionnaire respondents appeared to prefer the 1998 version more. In addition, this study offers several areas of improvement to the taxonomy that can help it become more widely accepted. This researcher also concluded that organizations responsible for the collection and distribution of Internet security information, do explicitly collect some, but not all, information useful as input into the taxonomy.

AN ANALYSIS OF THE COMPUTER AND NETWORK ATTACK TAXONOMY

I. Introduction

The Internet

> Nothing great was ever achieved without enthusiasm. Ralph Waldo
> Emerson (qtd. in Bartlett, 1980:497)

In 1957, the Soviet Union shocked the US with its launch of the Sputnik satellite.

This event convinced many in the US that despite its success during World War II and its

newfound position as the world leader, the US had lost its footing to the Soviet Union.

Therefore, in 1958 "Congress created the National Defense Education Act [...] essential

for the training of tomorrow's scientists" (Moschovitis, 1999:34). This act resulted in the

creation of the Advanced Research Projects Agency (ARPA) in 1958. ARPA, with

millions in government funds, led the research and development of computers and

information processing, to include the concept of "connecting computers across long

distances" (Ibid.).

By 1968, ARPA had become one of the premier research agencies in the world,

and a central point of contact for anyone doing research concerning communications,

computers, or information processing. However, sharing research information with all

these interested parties was still an arduous task, since the US Postal Service was still

the primary means used to transfer information from one area to another. This desire to

find a better way to share information lead to ARPA's goal of connecting computers

across long distances to allow the sharing of information. ARPA's breakthrough

occurred when it submitted requests for proposals to build Interface Message Processors (IMP) that would "connect the individual sites, route messages, scan for errors, and confirm the arrival of messages at their destinations" (Moschovitis, 1999:61). These IMPs became the building blocks for today's computer networks, and ultimately the Internet.

The birth of ARPAnet, which eventually became the Internet, occurred around September 1, 1969, in the shadow of the July 20, 1969 lunar landing. ARPA successfully networked IMPs located at the University of California at Los Angeles, the University of California at Santa Barbara, the University of Utah, and the Stanford Research Institute, thereby establishing the "foundation for advanced networking and breaks a path toward the Internet" (Moschovitis, 1999:61). However, this technological achievement received little fanfare, since the world still reveled in the lunar landing that occurred a few months earlier.

ARPA maintained control of the Internet for the next 20 years, with the DOD, research centers, and universities around the country as its primary users. In 1986, the National Science Foundation (NSF) expanded the ARPAnet by developing a network that allowed non-defense related users to be connected to the Internet (Moschovitis, 1999:125). The NSFnet dramatically increased the private sector's access to, and use of the Internet. The Internet community had grown beyond the wildest dreams of its developer, ARPA, and its maintainer, the US government. In an effort to keep pace with the demands on its use and to integrate evolving technology into the Internet, ARPA decommissioned ARPAnet in 1990, removed its original nodes from the Internet, and re-routed all traffic to the more robust and modern NSFnet backbone, maintained by the Michigan Educational Research Information Triad (MERIT), IBM and MCI (Abbate, 1999:196).

The NSFnet backbone opened Internet access to the commercial world. As the number of commercial users increased, so did the various types of uses of the Internet. The DOD, research centers, and universities quickly saw their exclusivity on the Internet disappear, as communications companies, computer companies, cutting edge businesses, entrepreneurs, and the public began getting connected. Although the US government still maintained control over the Internet, via the NSF, it began to encounter difficulty in maintaining the Internet in response to its growing user community. Therefore, the NSF relinquished control of the Internet to better facilitate the integration of new technologies. In 1994, the NSF issued a plan that would allow competitive Internet Service Providers (ISP) to operate their Internet service backbone and provide access to the public. These commercial backbones eventually became the replacement for NSFnet, thereby privatizing and commercializing the entire Internet. "On 30 April 1995, MERIT formally terminated the old NSFnet backbone, ending the US government ownership of the Internet" (Abbate, 1999:199). However, the Air Force's dependence on the Internet did not diminish due to its privatization and commercialization. In fact, it increased, along with the world's desire to be connected.

My January 1999, the US military had approximately one million hosts connected to the Internet (Moschovitis, 1999:278). A host is "any computer on a network that is a repository for services available to other computers on the network" (Department of the Air Force, *AFDIR33-303*, 1999:37). Describing the Air Force's increasing numbers of hosts connected to the Internet as extraordinary, may be extreme, however in relation to the growth of the Internet itself, it is not. Using *phenomenal* to describe the Internet may be an understatement, but it does capture the essence as represented by Figure 1:
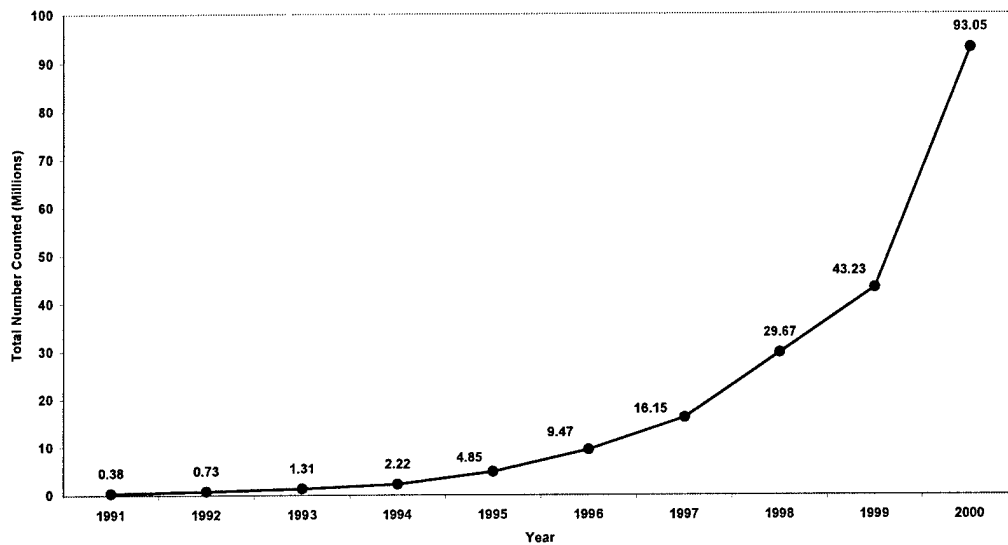
(ISC, *Internet Domain Survey: July 2000*, 2000)

Figure 1 - Growth of Internet via Number of Hosts Connected

In addition, the Internet phenomenon expands well beyond the US borders.

Originally designed to meet the needs of the DOD, the Internet now supports users from

around the world. The Information Age indicator, Internet hosts per 10,000 people, of

the World Development Indicators (WDI) 1999, clearly illustrates this expansion. Figure

2 graphically illustrates this data point.
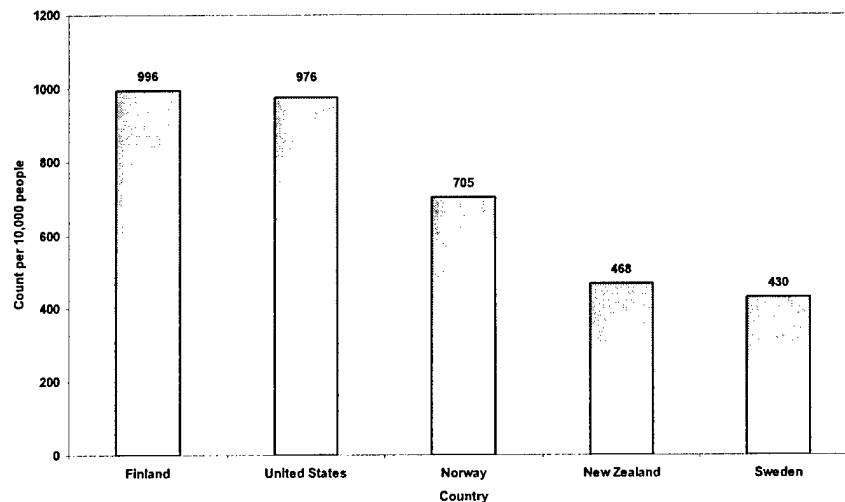
(WDI, 1999)

Figure 2 - Internet Hosts per 10,000 People (Top Five Countries), as of July 1998

4

Of course, the primary access method to the Internet, personal computers, experienced

phenomenal growth to match the growth of the Internet. Once again, the Information

Age indicator of the World Development Indicators 1999 clearly illustrates the extremely

large number of personal computers worldwide. Figure 3 graphically illustrates this data

point.
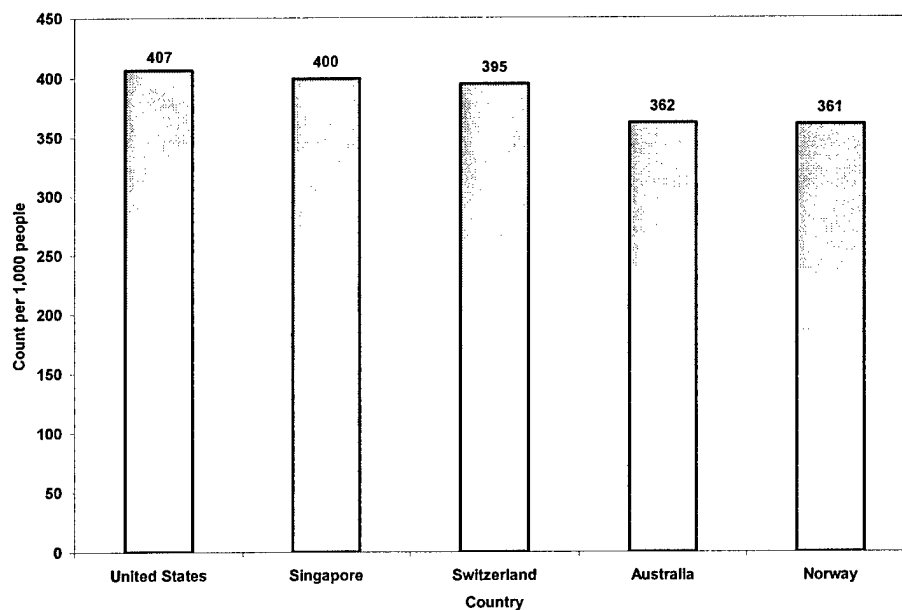
(WDI, 1999)

Figure 3 - Personal Computers per 1,000 People (Top Five Countries), as of 1998

The Internet provides seamless connectivity to networks throughout most of the

developed world, continues to grow at a phenomenal rate, and is the heart and soul of

the information technology era. However, it does not come without risk. John M.

Deutch, former Director of Central Intelligence Agency, stated this quite succinctly in his

1996 testimony to the US Senate Committee on Governmental Affairs, Permanent

Subcommittee on Investigations, "I, like many others in this room, am concerned that

this connectivity and dependency make us vulnerable to a variety of information warfare

attacks" (Deutch, 1996).

Information Superiority

> Information has long been an integral component of human competition—those with a superior ability to gather, understand, control, and use information have had a substantial advantage on the battlefield. (Department of the Air Force, *AFDD 2-5*, 1998:i)

The importance of information to warfighting led the Air Force to the realization that information is a crucial offensive and defensive resource. Along with land, sea, air, and space operations, information operations (IO) now constitutes the "fifth dimension of warfare" (Fogleman, 1995). In recognition of this distinction, the Air Force identified information superiority as a core competency. Information superiority is "the degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition" (Department of the Air Force, *AFDD 2-5*, 1998:2). The Air Force explicitly stated its commitment to information superiority by stating, "while Information Superiority is not the Air Force's sole domain, it is, and will remain, an Air Force core competency" (Department of the Air Force, *Global*, 1996). Figure 4 illustrates how the Air Force envisions the integrated components of information superiority:

```
            ┌──────────────────────────────────┐
            │     INFORMATION SUPERIORITY      │
            └──────────────────────────────────┘
                             │
                 ┌───────────────────────┐
                 │ Information Operations │
                 └───────────────────────┘
                             │
        ┌────────────────────┴────────────────────┐
┌─────────────────────────┐          ┌─────────────────────────┐
│ Information-in-Warfare   │          │   Information Warfare    │
└─────────────────────────┘          └─────────────────────────┘
Gain              Exploit             Attack              Defend
          ISR                         ┌─────────────────────────┐
        Weather                       │    Counterinformation   │
Precision Navigation & Positioning    └─────────────────────────┘
  Other Information Collection/
     Dissemination Activities
                          ┌─────────────────┐   ┌─────────────────┐
                          │    Offensive    │   │    Defensive    │
                          │ Counterinformation │ Counterinformation │
                          └─────────────────┘   └─────────────────┘
                             PSYOP              Information Assurance
                        Electronic Warfare            OPSEC
                        Military Deception       Counterintelligence
                         Physical Attack          Counter PSYOP
                        Information Attack      Electronic Protection
                                                  Counterdeception
```

(Department of the Air Force, *AFDD 2-5*, 1998:3)

Figure 4 - Air Force Information Superiority Construct

To successfully deploy a superiority strategy, Sun Tzu identified the following

"prerequisites for combat commanders" (Huang, 1993:66):

- Plan, but know the calculation of gains and losses
- Mobilize, but know the causes for action and inaction
- Control, but know lethal and safe terrains
- Fight, but know where there are sufficiencies and deficiencies

Since the Air Force considers IO a new dimension of war, and plans to implement an

information superiority strategy, these prerequisites should apply. Unfortunately, the

lack of quantifiable, repeatable method of describing Internet security risks in relation to

these prerequisites appears to be a weak link in Air Force's information superiority

strategy. Without this information, how can the Air Force effectively plan, mobilize, control, and fight in this new dimension?

To add to this weak link, the Air Force knows its adversaries are also working on IO strategies. According to Dr. Wess Roberts, author of Leadership Secrets of Attila the Hun, commanders should "not underestimate the power of an enemy, no matter how great or small, to rise against you on another day" (Roberts, 1985:58). The Air Force holds commanders accountable for the posture and execution of Defensive Counterinformation (DCI) within their commands. DCI "includes those actions that protect information, information systems, and information operations from any potential adversary" (Department of the Air Force, AFDD 2-5, 1998:10). Unfortunately, the free flowing nature of the Internet, added to the changing face of the threats, make commanders' jobs even harder. As stated in Air Force Doctrine Document 2-5 Information Operations (AFDD 2-5), "terrorists, criminals, and hackers are becoming more of a threat as they discover the benefits of using the electronic environment to accomplish their goals" (Department of the Air Force, AFDD 2-5, 1998:6).

The Problem

> My greatest concern is that hackers, terrorist organizations, or other nations might use information warfare techniques as part of a coordinated attack designed to seriously disrupt:
>
> - Infrastructures such as electric power distribution, air traffic control, or financial sectors;
> - International commerce; and
> - Deployed military forces in time of peace or war. (Deutch, 1996)

Mr. Deutch's words are very relevant today. As the Air Force's dependence on the Internet continues to grow, so do concerns about Internet security. Global Engagement: A Vision for the 21st Century Air Force, which is part of the National

Security Strategy, contains these unambiguous words in reference to the information superiority core competency:

> Information Operations, and Information Warfare (IW) in particular, will grow in importance during the 21st Century. The Air Force will aggressively expand its efforts in defensive IW as it continues to develop its offensive IW capabilities. The top IW priority is to defend our own increasingly information-intensive capabilities [...] on the offensive side, the Air Force will emphasize operational and tactical IW and continue, in conjunction with other Federal agencies, to support strategic information operations. (Department of the Air Force, *Global Engagement*, 1996)

The Air Force provides even more reasons to develop a reliable, repeatable process to classify Internet security incidents because of its goal for Internet use within the service. According to the Air Force Instruction 33-129 Transmission of Information via the Internet, "the Air Force goal for the Internet is to provide maximum availability at acceptable risk levels for Air Force members needing access for the execution of official business" (Department of the Air Force, *AFI 33-129*, 1999:3). Therefore, developing a process to classify Internet security incidents must advance beyond scientific guesses. The Air Force should support and encourage sound research to ensure it, as well as its members, recognizes Internet security incidents and can classify them accordingly.

In 1997, John D. Howard submitted his dissertation, An Analysis of Security Incidents on the Internet 1989 – 1996, to Carnegie Mellon University as part of his requirements for the Doctor of Philosophy degree in Engineering and Public Policy. Howard explained that he was curious about the Internet and its security because many reputable people had stated that the Internet, although wondrous, was very insecure and dangerous. Yet, it was hard to find quantifiable evidence to support this fact. Thus, Howard began his research based on the premise:

> Security *is* a problem on the Internet. The thousands of successful break-ins over the years are a testimony to that. But just how much of a problem is it? The answer to this question is important for two reasons. First, with information about Internet security problems, we could determine to what

9

extent, and in what areas, government programs and policies should be instituted to devote society's resources to protecting the Internet. Second, trends over time could be used to determine the effectiveness of these policies and resources. (Howard, *Analysis*, 1997:1)

However, as Howard embarked on his research, he discovered that although many lists

of terms, lists of categories, tables, matrices, and taxonomies existed focusing on

computer and network attacks, they proved inadequate for his needs. According to

Howard:

> The taxonomy developed as part of this research is broader in scope than Landwher, et al., because it does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather attempts to provide a broad, inclusive framework. The intention was to reorient the focus of the taxonomy toward a process, rather than a single classification category, in order to provide both an adequate classification scheme for Internet attacks, and also a taxonomy that would aid in thinking about computer and network security. (Howard, *Analysis*, 1997:60)

Eventually, Howard developed his computer and network attack taxonomy shown in

Figure 5.

Attackers	Tools	Access					Results	Objectives
Hackers	User Command	Implementation Vulnerability	Unauthorized Access			Files	Corruption of Information	Challenge, Status
Spies	Script or Program	Design Vulnerability	Unauthorized Use	Processes	Data in Transit		Disclosure of Information	Political Gain
Terrorists	Autonomous Agent	Configuration Vulnerability					Theft of Service	Financial Gain
Corporate Raiders	Toolkit						Denial-of-service	Damage
Professional Criminals	Distributed Tool							
Vandals	Data Tap							

(Howard, *Analysis*, 1997:73)

Figure 5 - 1997 Computer and Network Attack Taxonomy

Although Howard's taxonomy focused on attacks, he subsequently used his

taxonomy to classify incidents during his study. He defined attacks as "a single

unauthorized access attempt, or unauthorized use attempt, regardless of success"

10

(Howard, *Analysis*, 1997:287) and defined incidents as "a group of attacks that can be

distinguished from other incidents because of the distinctiveness of the attackers, and

the degree of similarity of sites, techniques, and timing" (Ibid.:289). However, more

important is that the taxonomy was developed from:

> [...] a *process* or *operational* viewpoint. From this viewpoint, an *attacker* on
> computers or networks attempts to link to ultimate *objectives* or motivations.
> This link is established through an operational sequence of *tools*, *access*,
> and *results* that connects these attackers to their objectives [...] (Ibid.:71)

Therefore, Howard's taxonomy is more than a listing of information, its attempts to

describe the process of computer and network attacks.

Approximately one year after publishing his dissertation containing the original

computer and network attack taxonomy, Howard and Longstaff published a new version,

illustrated in Figure 6, in the 1998 Sandia National Laboratories Report titled A Common

Language for Computer Security Incidents. According to Howard and Longstaff:

> Finally, it is hoped that by demonstrating the utility of this particular
> representation for incident data, other response teams could structure
> incident in the same taxonomy, facilitating the sharing of information and
> allowing a more complete and accurate analysis of security incidents
> across a wider range of victimized sites. (Howard and Longstaff, 1998:19)

Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge, Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

(Howard and Longstaff, 1998:16)

Figure 6 - 1998 Computer and Network Attack Taxonomy, 1998

This thesis examines the computer and network attack taxonomies developed by Howard. Howard developed the taxonomies to help him classify Internet security attacks and incidents as part of his doctoral research and as part of a follow-on project to help develop a common language for the computer security. A resulting recommendation included continued evaluation of the computer and network taxonomies to make practical modifications. This continued evaluation may lead to its wider acceptance by the Internet security community, as well as maintain the taxonomies' currency due to the dynamic nature of the Internet. In addition, this analysis exposes the Air Force to a possibly better method to classify Internet security attacks and incidents. Finally, this thesis adds to the body of knowledge with respect to Internet security and other related

disciplines, such as computer security, information security, communication security, information assurance, and information warfare.

Research Overview

The remaining chapters of this thesis provide the details of this research. Chapter II contains the literature review, which explores the existing body of knowledge pertinent to this research topic. Chapter III describes the method used and assumptions made while analyzing the data. Chapter IV provides the findings of the analysis performed on the data. Finally, Chapter V discusses the findings, presents conclusions, and makes recommendations for further research in this area.

II. Literature Review

If it keeps up, man will atrophy all his limbs but the push-button finger.
Frank Lloyd Wright (qtd. in Quoteland.com, 2000)

The Internet and Society

As indicated by Figure 1, Figure 2, and Figure 3, the phenomenal growth of the

Internet means that people, states, and countries believe in this information technology

resource. The Internet, the information superhighway, provides the backbone for the

electronic exchange of information around the world, with the US being a major user and

developer. According to the Science & Engineering Indicators – 2000 compiled by the

National Science Board (NSB), "the revolution in information technology (IT) has been

likened to the industrial revolution in terms of its potential scope" (NSB, 2000:9-4). The

NSB is:

> Responsible, by law, for developing on a biennial basis, a report "[...] on
> indicators of the state of science and engineering in the United States."
> The Science and Engineering Indicators series was designed to provide a
> broad base of quantitative information about U.S. science, engineering, and
> technology for use by public and private policymakers. (NSB, 2000:xiv;
> NSF, 2000)

The NSB recognized the impact of IT to American society and dedicated an entire

chapter of the Science & Engineering Indicators – 2000 to the subject.

The NSB defined IT as an integration of "three key technologies: digital

computing, data storage, and the ability to transmit digital signals through

telecommunications networks" (NSB, 2000:9-5). The statistics generated by the NSB

gives credibility to the existence of an IT revolution. The NSB clearly states that:

> The U.S. economy approaches the end of the 20th century with
> unprecedented real growth, miniscule inflation, low un-employment, and
> strong consumer and investor confidence. Economists have dubbed it the
> "Cinderella economy." The reasons for this success are many and varied.

However, it can be argued that technological change has been behind the economic boom of the late 1990s. (NSB, 2000:2-6)

The NSB broadened the scope of IT by using the term high technology, as defined by the Organisation for Economic Co-operation and Development (OECD). The OECD contains 29 member countries, which includes the US, and is "an organisation that, most importantly, provides governments a setting in which to discuss, develop and perfect economic and social policy" (OECD, 2000). The OECD identified four industries as high technology based on their research and development (R&D) intensities: aerospace, computers and office machinery, electronics-communications, and pharmaceuticals" (NSB, 2000:7-4; Sakurai, Evangelos, and Papaconstantinou 1996:38).
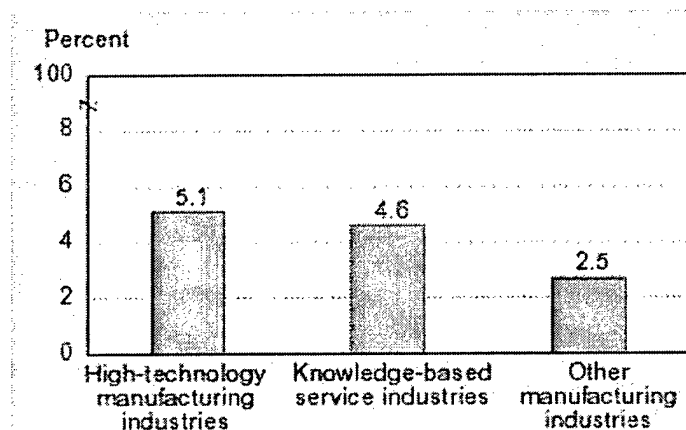
(NSB, 2000:7-6)

Figure 7 - Avg. Annual Rates of Growth in Three U.S. Economic Sectors: 1980 - 97

This high technology sector experienced the most growth during the past two decades, as illustrated by Figure 7. More importantly, three of the industries that comprise high technology, aerospace, computers and office machinery, and electronics-communications, play substantial roles in the defense industry.

Figure 8 illustrates more vividly the influence high technology industries have on the current US economic boom. Venture capital firms invested $16.8 billion dollars in 1998. High technology firms that developed computer software or offered software

services garnered top billing by receiving 33 percent of the investments.

Telecommunications firms were second, receiving 17 percent of the investments (NSB, 2000:7-3).

Biotechnology
Communications
Computer hardware
Consumer related
Industrial/energy
Medical/health
Semiconductors/ other electronics
Software & services
Other products/ services

☐ 1988
■ 1998

0   10   20   30   40   100

Percentage of total venture capital disbursements
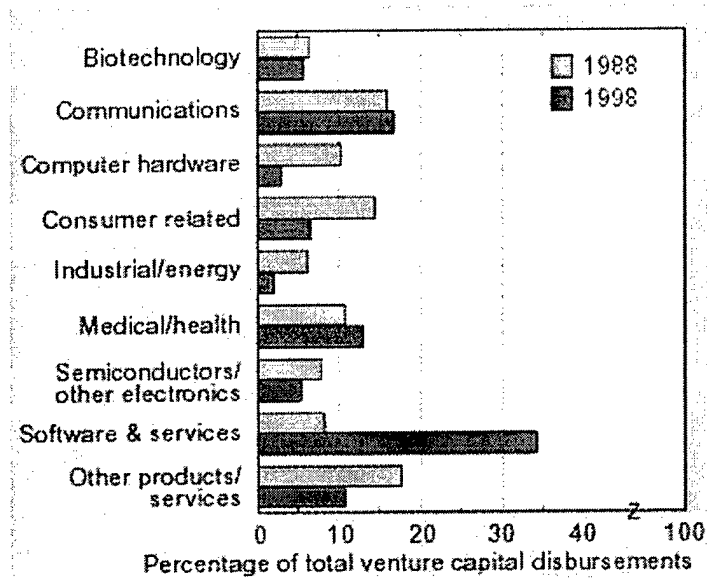
(NSB, 2000:7-25)

Figure 8 - U.S. Venture Capital Disbursements, By Industry Category: 1988 & 1999

In short, the Science & Engineering Indicators – 2000 clearly illustrate that:

> The United States continues to lead or be among the leaders in all major technology areas. Advancements in information technologies (computers and telecommunications products) continue to influence new technology development and to dominate technical exchanges between the United States and its trading partners. (NSB, 2000:7-3)

The NSB provided a more succinct comment on the impact of information technology, "information technology has had an impact on virtually all sectors of our economy and society, including the conduct of research, as well as our daily lives" (NSB, 2000:1-39).

The economic status of the US clearly shows that high technology industries played a major role in the current economic boom. Yet, they do not indicate the role the Internet played. The term Internet is a "catch-all term used to describe the massive worldwide network of computers. Literally it means network of networks, and is a

16

worldwide interconnection of individual networks operated by government, industry, academia, and private sectors" (Department of the Air Force, *AFDIR33-303*, 1999:105). Due to the nebulous nature of the Internet, quantifying its role in the current economic boom is difficult. However, the NSB does predict that:

> Technological change is expected to continue to transform many aspects of economic production, distribution, and consumption. Such changes include, for example, further development of Internet commerce (e.g., banking and retail operations), additional advances in biotechnology (e.g., "designer" drugs), greater automation in production (e.g., advanced robotic systems), new forms of household entertainment (e.g., digital video disc entertainment systems), and new ways of conducting scientific research itself (e.g., the creation of virtual laboratories). (NSB, 2000:2-6)

Consequently, if indicators show that high technology is the juggernaut behind the US' current economic boom, to include the Internet, then analyzing Internet security to maintain society's confidence in this technology such be of utmost importance. Part of this analysis includes the ability to clearly and consistently identify security issues and threats.

Although the statistics referenced thus far provide a telling story on the impact of the Internet in the US, the statistics derived from the population at large provides a more breathtaking picture. The NSB documented several Internet related trends, which includes:

- Internet-based electronic commerce is growing rapidly and changing the impact of IT on the economy. Private market research firms estimated that the value of transactions conducted over the Internet will reach $1 trillion by 2003 (up from $40-100 billion in 1998). (NSB, 2000:9-3)

- Schools are rapidly connecting to the Internet. By 1998, 89 percent of public schools were connected to the Internet (up from 35 percent in 1994). (Ibid.:93)

- Colleges are increasingly using IT in instructions. The percentage of college courses using e-mail, Internet resources, class Web pages, and other forms of information technology in instruction increased rapidly between 1994 and 1998. (Ibid.:93)

- Governments around the world are using the Internet and the World Wide Web to communicate with constituencies. ((Ibid.:93)

Additional trends clearly indicate that US citizens consider the Internet a staple ingredient in their homes and work centers. For example, "the number of people without access to a computer either at home or at work fell substantially between 1983 and 1999—from 70 percent down to 34 percent" (NSB, 2000:8-2). Furthermore, the increased access to computers in homes and work centers also increased Internet and computer usage, as illustrated in Figure 9.
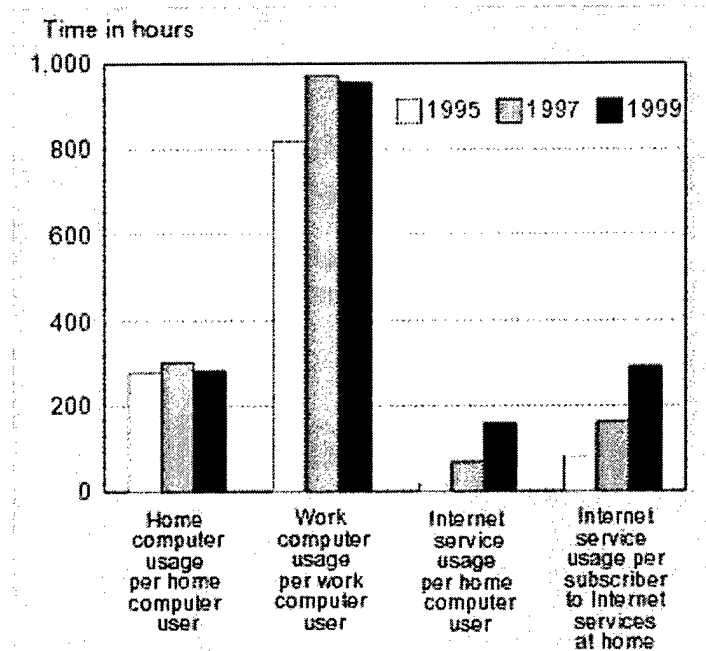
(NSB, 2000:8-24)

Figure 9 - Computer Usage: Average Hours Per Year: 1995, 1997, 1999

The Internet, without doubt, plays an important role for many Americans. It may be difficult to quantify its importance, however the Science & Engineering Indicators – 2000 implies that it is very important:

- In 1999, for the first time ever, a majority (54 percent) of American adults had at least one computer in their homes. (NSB, 2000:8-2)
- Approximately one-third of Americans subscribed to an on-line service and had home e-mail addresses in 1999. (Ibid.:8-2)

18

Since American society places such a high value on access to the Internet, Internet

security has inevitably become important too. Along that line, since the DOD protects

and defends the US from all enemies, foreign and domestic, the DOD must address

Internet security since it has now become a valued domestic resource. More

specifically, the Air Force must address Internet security since the Air Force considers

the Internet a valued resource too, as it continues to integrate the Internet into its daily

worldwide operations.

The Internet and the Air Force

According to Global Engagement: A Vision for the 21st Century Air Force, the post-

Cold War Air Force considers "information as a weapon/target" (Department of the Air

Force, *Global Engagement*, 1996). The Air Force considers information such a valuable

weapon/target, that it added information superiority as a core competency. The Air

Force stated:

> Today, more than ever, gaining and maintaining information superiority is a
> critical task for commanders and an important step in executing the
> remaining Air Force core competencies. The execution of information
> operations in air, space, and, increasingly, in "cyberspace" constitutes the
> means by which the Air Force does its part to provide information
> superiority to the nation, joint force commander, and Service component
> and coalition forces. (Department of the Air Force, *AFDD 2-5*, 1998:i)

The Air Force's belief in information superiority resulted in it developing its own

construct, as illustrated in Figure 4, to pursue, achieve, and integrate information

superiority into other aspects of the Air Force environment.

Although the Air Force Information Superiority Construct explicitly affects the Air

Force's information systems, the Air Force realizes that the information infrastructure

"transcends industry, the media, and the military and includes both government and

nongovernment entities" (Department of the Air Force, *AFDD 2-5*, 1998:4). The term

19

information infrastructure refers to the link between "individual information systems through numerous and redundant direct and indirect paths, including space-based systems" (Ibid.:4). These redundant direct and indirect paths include the Internet. The Air Force more narrowly defines the components of the Internet that supports its mission as the Defense Information Infrastructure (DII), the National Information Infrastructure (NII), and the Global Information Infrastructure (GII).

The DII is:

> The web of communications networks, computers, software, databases, applications, and other services that meet the information processing and transport needs of DOD users, across the range of military operations. The DII includes the information infrastructure of the Office of the Secretary of Defense, the military departments, the Chairman of the Joint Chiefs of Staff, the Defense agencies, and the combatant commands. It provides information processing and services to subscribers over the Defense Information System Network and includes command and control, tactical, intelligence, and commercial communications systems used to transmit DOD information. The DII is embedded within and deeply integrated into the National Information Infrastructure. Their seamless relationship makes distinguishing between them difficult. (Department of the Air Force, *AFDIR 33-303*, 1999:75)

The DII transcends the US military and civilian sectors, which is a compelling reason to why analyzing Internet security activity is so important. How does this compare to the NII?

The NII is:

> The nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of communications and information equipment, systems, and networks, including the personnel who make decisions and handle the transmitted information. The NII is similar in nature and purpose to the Global Information Infrastructure but relates in scope only to a national information environment, which includes all government and civilian information infrastructures. (Department of the Air Force, *AFDIR 33-303*, 1999:119-120)

Similar to the DII, the NII's definition reiterates the tight coupling of the government and

public information resources. The interrelationship between the DII and NII leads to the

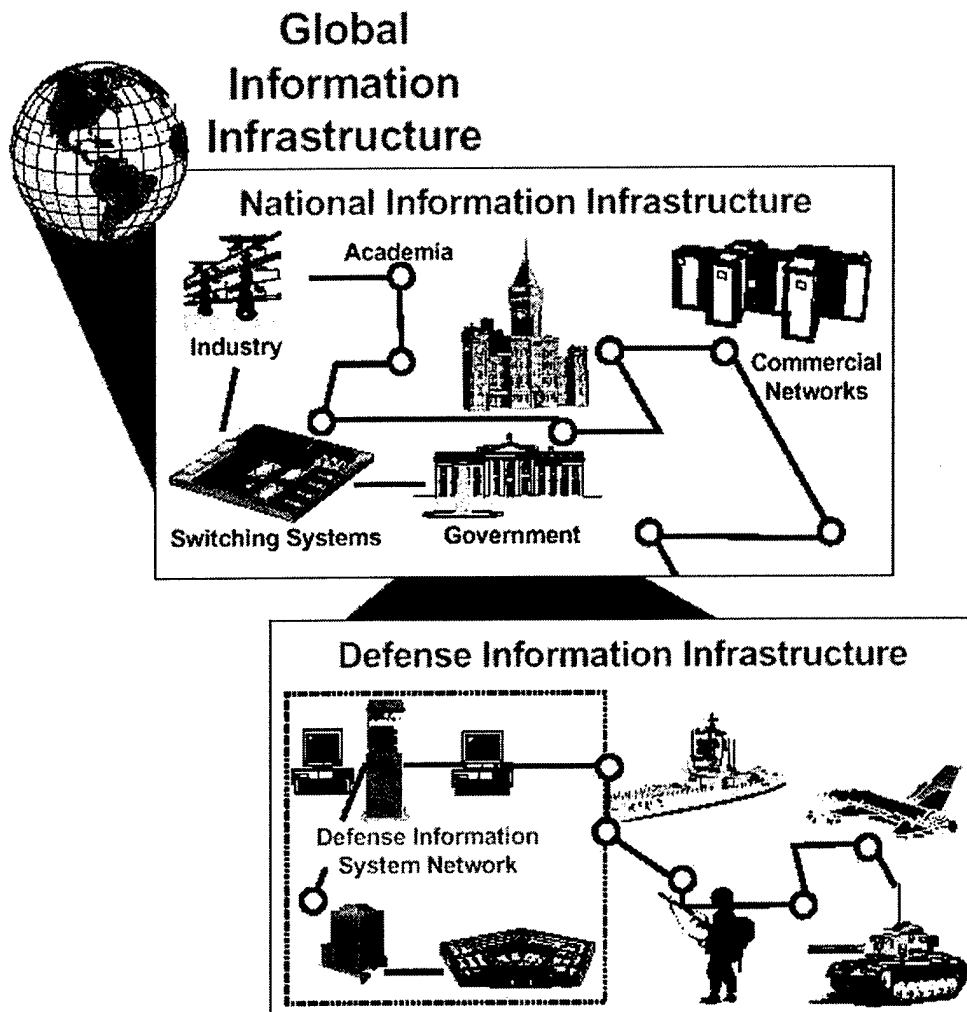next level of information infrastructure integration, the GII.

The GII is:

> The worldwide interconnection of communications networks, computers,
> databases, and consumer electronics that make vast amounts of
> information available to users. It encompasses a wide range of
> communications and information equipment, systems, and networks, to
> include the personnel who make decisions and handle the transmitted
> information. (Department of the Air Force, *AFDIR 33-303*, 1999:94)

The DII definition uses the word *web* as a metaphor for the interconnectivity provided by

the Internet. The NII and GII actually include *interconnection* within their definition,

which also refers to the Internet. Therefore, the Internet, from the Air Force's

perspective, consists of the interconnected DII, NII, and GII, as illustrated in Figure 10.

These information infrastructures provide the worldwide connectivity used by the Air

Force to accomplish its mission.

Global Information Infrastructure

National Information Infrastructure

Academia

Industry

Commercial Networks

Switching Systems   Government

Defense Information Infrastructure

Defense Information System Network

(JCS, 1998:I-14)

Figure 10 - DII, NII, and GII Interfaces

An insecure Internet as illustrated by Figure 10, poses a threat to the Air Force.

AFDD 2-5 provided the following description of the interaction between the DII, NII, and

GII:

> In reality, a news broadcast, a diplomatic communiqué, and a military
> message ordering the execution of an operation all depend on the GII.
> (Department of the Air Force, *AFDD 2-5*, 1998:5)

Therefore, any breach of security, any vulnerability that an adversary can use to its

advantage to disrupt or taint this order, can cause untold damage to the US and its

22

Allies. Thus, analyzing Internet security incidents to clearly and consistently identify threats gain importance as the Air Force becomes more dependent on the Internet.

Information systems and the Internet provide a new dimension of warfare for the Air Force. It provides a mechanism and equalizer for our adversaries too, especially the less advanced and wealthy, to take action against the US. For the cost of a personal computer and Internet access, along with the desire and the technological knowledge, advisories worldwide can exploit known Internet vulnerabilities to harm the US, as illustrated in Figure 11:

(JCS, 1998:I-16)
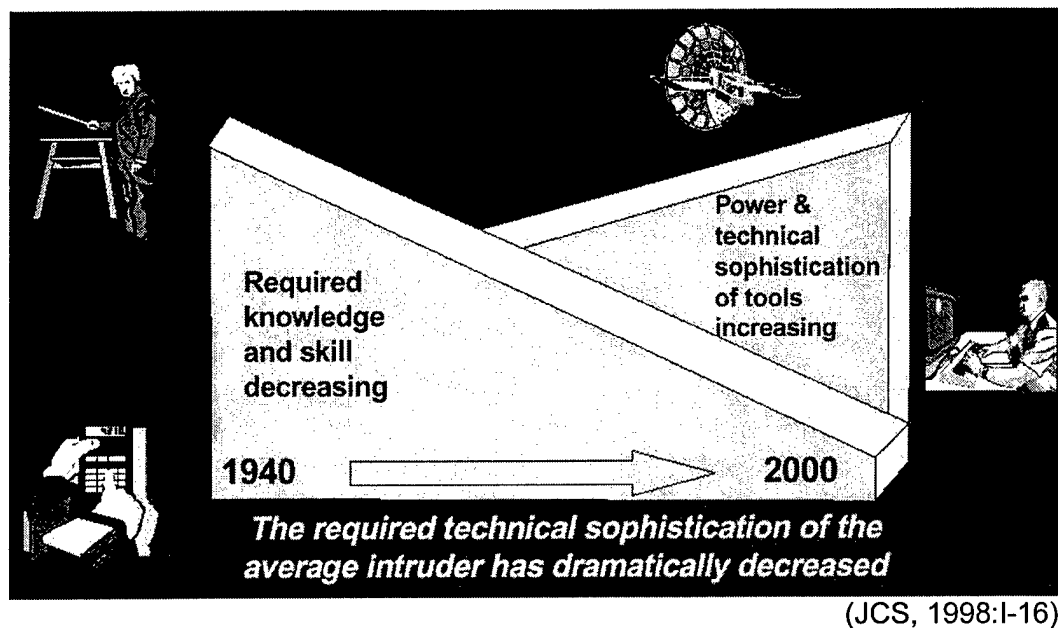
Figure 11 - Emerging IO and Technology

The Air Force voiced its concerns about this issue by stating:

> Just as the United States plans to employ IO against its adversaries, so too can it expect adversaries to reciprocate. Numerous countries have discovered the benefits of IO. They employ psychological operations (PSYOP), electronic warfare (EW), and military deception and now are collecting available intelligence via the Internet and creating malicious code and hacking cells. Terrorists, criminals, and hackers are becoming more of a threat as they discover the benefits of using the electronic environment to accomplish their goals. (Department of the Air Force, *AFDD 2-5*, 1998:6)

23

The Air Force should be concerned about these threats, since the DII, NII, and GII all represent portions of the Internet.

These threats continue to concern the Air Force. Table 1 lists threats that the Air Force believes pose risks to systems that rely on information technology. These threats pose risks for "both stand-alone and networked weapon and support systems [...] these threats can be employed by both organized entities, such as nation-states, and unstructured threats, such as rogue computer hackers" (Department of the Air Force, *AFDD 2-5*, 1998:7).

Table 1 - Information Warfare Threats

Compromise	Deception/ Corruption	Denial/Loss	Destruction
• Malicious Code • System Intrusion • Psychological Ops • Intel Collection • Technology Transfer • Software Bugs	• Malicious Code • System Intrusion • Military Deception • Spoofing • Imitation	• Malicious Code • Bombs • Directed Energy • Weapons • Lasers • Physical Attack • Nuclear & Non-nuclear EMP • Chemical/ • Biological • Warfare	• System Intrusion • Lasers • Physical Attack • Nuclear & Non-nuclear EMP • Virus Insertion • System Overload • Radio Frequency • Jamming

(Department of the Air Force, *AFDD 2-5*, 1998:6)

Once again, the information warfare threats do not explicitly mention the Internet, however the many of the information warfare threats can occur via the Internet.

The risks posed by the information warfare threats provide enough motivation to develop a process to clearly and consistently classify Internet security attacks and incidents. According to Global Engagement: A Vision for the 21st Century:

> Information Operations, and Information Warfare (IW) in particular, will grow in importance during the 21st Century. The Air Force will aggressively expand its efforts in defensive IW as it continues to develop its offensive IW capabilities. The top IW priority is to defend our own increasingly information-intensive capabilities.

Nevertheless, the Air Force provides another motivator with respect to its focus on defensive counterinformation (DCI). DCI includes information assurance, operational security, counterdeception, counterintelligence, counterpsychological operations, and electronic protection. According to AFDD 2-5, "DCI is the Air Force's overall top priority within the information warfare arena. Commanders are accountable for DCI posture and execution within their commands" (Department of the Air Force, *AFDD 2-5*, 1998:7). Therefore, this statement implies that Internet security should also be a top priority not only for the Air Force generally, but for Air Force commanders specifically. As such, being able to clearly and consistently identify the threats to Air Force information and information systems is a necessity.

As the Air Force continues to integrate its daily operations with the Internet, analyzing Internet security incidents becomes more important. The Air Force Research Laboratory in Rome, New York recently announced its participation in the DOD's $50 million research project of the Next Generation Internet (NGI). In his explanation of the purpose of the NGI, Secretary of Defense William Cohen reiterated the importance of the Internet to the military and the public:

> "Internet technology was first demonstrated by the military in the 1970s and is the foundation of today's military and commercial network systems," said Secretary of Defense William Cohen. "The military must stay ahead in information technologies to dominate in the future. The Next Generation Internet program will enable revolutionary capabilities of importance to both the Department of Defense and the nation as a whole." (AFN, *AFRL*, 2000)

Therefore, analyzing Internet security incidents, with respect to the current technology, will be helpful as the Air Force participates in the development of the NGI.

The Research Agenda

Given the growing dependence upon the Internet by the American citizens in general, and the Air Force in particular, the body of knowledge that addresses Internet security remains small. To address this issue, which crosses the boundaries of several areas of expertise, such as, computer and communications security, software engineering, fault-tolerance, systems design and implementation, and networking, among others, the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA) charted the Committee on Information Systems Trustworthiness. DARPA and the NSA requested the committee to "examine, discuss, and report on interrelated issues associated with the research, development, and commercialization of technologies for trustworthy systems and to use its assessment to develop recommendations for research to enhance information systems trustworthiness" (Schneider, et al, 1999:viii). The committee included experts from the previously listed areas of expertise, as well as the Computer Science and Telecommunications Board, the Commission on Physical Sciences, Mathematics, and Applications, and the National Research Council; a who's who in information technology and research.

The Committee on Information Systems Trustworthiness focused on networked information systems (NIS). The Committee defined NIS as integrated "computing systems, communications systems, people (both as users and operations); procedures, and more" (Schneider, et al, 1999:2). It also defined trustworthiness as:

> Assurance that a system deserves to be trusted—that it will perform as expected despite environmental disruptions, human and operator error, hostile attacks, and design and implementation errors. Trustworthy systems reinforce the belief that they will continue to produce expected behavior and will not be susceptible to subversion. (Ibid.:316)

The primary NISs subjected to this study were the public telephone system (PTN) and the Internet due to their extremely large size, dependence upon each other, society's dependence upon the PTN, and society's growing dependence upon the Internet.

The committee openly admits that the title of their final report, Trust in Cyberspace, is intentionally ambiguous. The report notes:

> One reviewer, contemplating the present, suggested that a question mark be placed at the end of the title to raise questions about the trustworthiness of cyberspace today. And this is a question that the report does raise. (Schneider, et al, 1999:viii)

Regardless of the interpretation of the title's meaning, one of the conclusions developed by the committee was that more research is needed in this area. They offered several conclusions and recommendations pertinent to this study, and future studies, into the overarching area of information technology in their final report, published in 1999:

- [...] absent scientific studies that measure dominant detractors of NIS trustworthiness, it its hard to know what vulnerabilities are the most significant or how resources might best be allocated in order to enhance a system's trustworthiness. (Schneider, et al, 1999:15)

- Rigorous empirical studies of systems outages and their causes are a necessary ingredient of any research agenda intended to further NIS trustworthiness. (Ibid.:15)

- Security research during the past few decades has been based on formal policy models that focus on protecting information from unauthorized access by specifying which users should have access to data or other systems objects. It is time to challenge this paradigm of "absolute security" and move toward a model built on three axioms of insecurity: insecurity exists; insecurity cannot be destroyed; and insecurity can be moved around. (Ibid.:247)

- The premise of this report is that a "trust gap" is emerging between the expectations of the public (along with parts of government) and the capabilities of NISs. (Ibid.:21)

- Hostile attacks are the fastest-growing source of NIS disturbances. Indications are that this trend will continue and that, because they can be coordinated attacks are potentially the most destabilizing form of trustworthiness breach. (Ibid.:22)

- A few university computer science departments have several faculty members who emphasize computer security research, but many departments have none who do. In any event, the number of computer security researchers is small compared to the number in other specialties [...]. (Ibid.:235).

- DARPA is generally effective in its interactions with the research community, but DARPA needs to increase its focus on information security and NIS trustworthiness research, especially with regard to long-term efforts. (Ibid.:254)

- An increase in expenditures for research in information security and NIS trustworthiness is warranted. (Ibid.:255)

As illustrated by the previous information, American society's dependence on the Internet continues to grow, as well as Air Force's dependence. However, the scientific and empirical research required identify and classify security issues continue to lag. "Articulating an agenda for that research" (Schneider, et al, 1999:13) was a goal of the Committee on Information Systems Trustworthiness. Beneficiaries of this agenda include researchers, policymakers, NIS operators, and product developers, all of whom have a stake in the findings resulting from this research agenda.

The Reality of Internet Security Incidents

Given the growing dependence on the Internet and the lack of research focused on Internet security activity, how can one determine the prevalence of Internet security incidents? Due to national security concerns by the DOD and liability concerns of the public, quantifying an answer remains elusive. However, by gleaning publicly accessible resources, it certainly suggests that a problem exists. Table 2 provides some insight into Internet security incidents. Obviously, the list is not all-inclusive. Nonetheless, it does illustrate that all Internet users are potential victims of Internet security incidents and the Air Force would not be the sole beneficiary of analyzing these events.

28

Table 2 - List of Publicly Known Internet Security Incidents

| Internet Security Incident	Description	Source
Air Force home page hacked	Vandalism and data destruction	(AFN, *Hacker*, 2000)
Computer attacks	Numerous computer attacks via the Internet against DOD computer systems occur daily.	(GAO, *T-AIMD-96-92*, 1996)
Computer based crimes	Various hacking, data mischief, theft and copyright violations occur via the Internet	(AFN, *Theft*, 2000)
Distributed-Denial-of-Service (DDOS) attacks on commercial websites	Intentional attack on commercial web sites that denied access to legitimate users and customers.	(Abreu, 2000; Frank, 2000)
Federal website attacks and vandalism	Vandalism, defacing, and distributed-denial-of-service to various Federal web sites	(GAO, *T-AIMD-99-223*, 1999)
ILOVEYOU virus	Destructive email virus that does various damage to infected computers	(GAO, *T-AIMD-00-171*, 2000)
Intrusions	Various DOD computers victim of unauthorized access attempts	(AFN, *DOD*, 2000)
IO attack	Speculation that the US conducted IO attacks against Serbia and Kosovo during 78-day war in 1999	(Brewin, 1999)
Melissa virus	Destructive macro virus that affected Microsoft Word 2000 and Word 97.	(GAO, *T-AIMD-99-146*, 1999)
Public posting of computer hacker tools	The availability of computer hacker tools on the Internet continues to grow	(GAO, *T-AIMD-96-108*, 1996)
Ramstein Air Base, Germany website hacked	Vandalism and defacing of website	(AFN, *Hacker*, 2000)
Solar Sunrise incident	Four days of hacker intrusions into DOD computer systems	(United States Senate, 1998)
Use of Zombies during DDOS attacks	Hijack of commercial servers which are then used to conduct DDOS attacks	(Verton, 2000:10)
Various hacker intrusions	DOD computer systems victim on continuous hacker attacks	(GAO, *AIMD-98-22*, 1999)

In addition, three studies depict the realities of Internet security incidents

concerning the DOD, the AF, and the general population. These studies were the

Defense Information Systems Agency (DISA) Vulnerability Analysis and Assessment

Program, the Air Force Information Warfare Center (AFIWC) Computer Security

Assistance Program (CSAP), and the Howard study, <u>An Analysis of Security Incidents</u>

<u>on the Internet 1989 – 1995</u>.

<u>GAO AIMD-96-84 Information Security: Computer Attacks at Department of</u>

<u>Defense Pose Increasing Risk</u>, published in 1996 and submitted to the US Senate

Committee on Governmental Affairs, reports on "the extent to which Defense computer

systems are being attacked, the actual and potential damage to its information and

systems, and the challenges Defense is facing in securing sensitive information" (GAO,

AIMD-96-84, 1996:1). The report based its facts on DISA's Vulnerability Analysis and

Assessment Program, in which DISA personnel penetrated DOD computer systems via

the Internet, from 1992 through 1995. The report stated:

- DISA conducted 38,000 total attacks
- DISA successfully gained access to 24,700 target computers, or 65 percent
- Total number of successful attacks detected, 988 or 4 percent
- Total number of detected attacks reported, 267 or 27 percent
- About 1 in 150 successful attacks drew an active defensive response from the organizations being tested (GAO, *AIMD-96-84*, 1996:19)

Figure 12 graphically illustrates the study's findings.
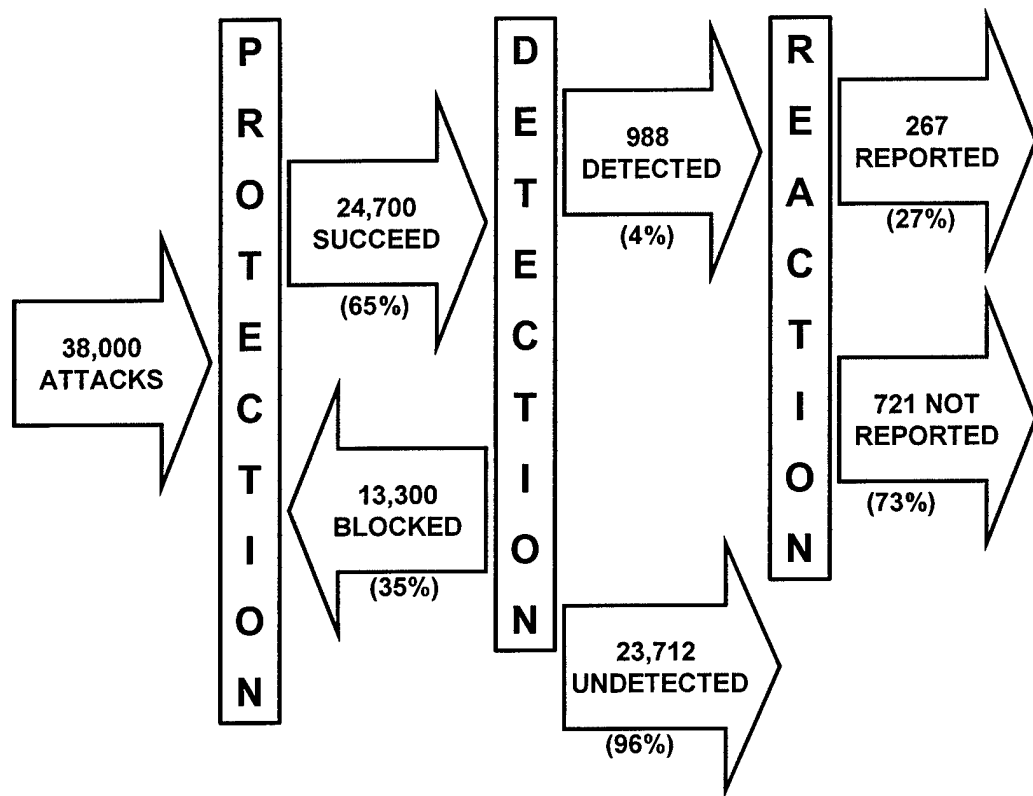
(GAO, *AIMD-96-84*, 1996:20)

Figure 12 - Results of DISA Vulnerability Assessments, 1992 – 1995

With respect to the AFIWC CSAP study, Howard stated that the AFIWC study was:

> [...] a different study during 1995, the "security posture" of selected systems at 15 Air Force bases was evaluated by the Air Force Information Warfare Center (AFIWC), as part of their Computer Security Assistance Program (CSAP) [...]. Of the 1,248 hosts attacked, 673 (54%) did not allow access. Access was gained at the root level on 291 hosts (23%), and to the account level on 284 hosts (23%). Of the 1,248 attacks, 156 were reported (13%), which means that around 1 out of every 8 attacks resulted in a report. (Howard, *Analysis*, 1997:175)

Figure 13 graphically illustrates the study's findings.
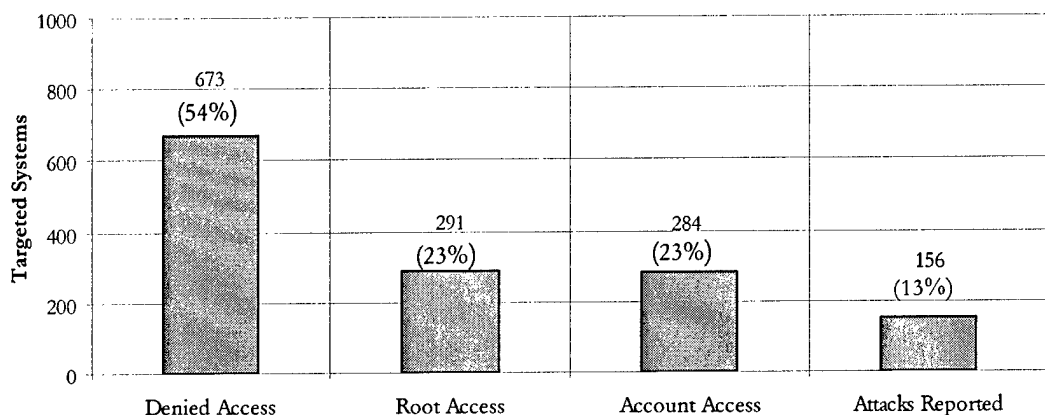
(White and Kincaid, 1996)

Figure 13 - AFIWC 1995 CSAP Results

Finally, Howard "analyzed trends in Internet security through an investigation of

4,299 security-related incidents on the Internet reported to the Computer Emergency

Response Team Coordination Center (CERT®/CC) from 1989 to 1995" (CERT®/CC,

Analysis, 2001). The CERT®/CC is:

> Located at the Software Engineering Institute (SEI), a federally funded
> research and development center at Carnegie Mellon University in
> Pittsburgh, Pennsylvania. Following the Internet Worm incident, which
> brought 10 percent of Internet systems to a halt in November 1988, the
> Defense Advanced Research Projects Agency (DARPA) charged the SEI
> with setting up a center to coordinate communication among experts
> during security emergencies and to help prevent future incidents. Since
> then, the CERT®/CC has helped to establish other response teams and
> our incident handling practices have been adopted by more than 85
> response teams around the world. (CERT®/CC, *Meet*, 2000)

Upon completion of his analysis, Howard found the following with respect to Internet

security activity:

> A total of 4,567 incidents over this 7 year period were
> reconstructed from the CERT®/CC records. This included 268 false
> alarms (5.9%), and 4,299 actual incidents (94.1%). Most of the
> CERT®/CC incidents (89.3%) were unauthorized access incidents, which
> were further classified into their degree of success in obtaining access:
> root break-in (27.7%), account break-in (24.1%), and access attempts
> (37.6%). Relative to the growth in Internet hosts, each of these access
> categories was found to be decreasing over the period of this research:
> root-level break-ins at a rate around 19% less than the increase in

Internet hosts, account-level break-ins at a rate around 11% less, and access attempts at a rate around 17% less.

Of the 4,299 actual incidents reported to the CERT®/CC, 458 (10.7%) were classified as unauthorized use incidents. These were further classified into denial-of-service attacks (2.4%), corruption of information incidents (3.1%), and disclosure of information incidents (5.1%). The growth in total unauthorized use incidents was around 9% per year greater than the growth in Internet hosts. (Howard, *Analysis*, 1997:235)

These studies provide a snapshot of the Internet security activity, from the DOD, Air Force, and public's perspective, from 1989 through 1995. Still, as illustrated by the following examples, analyzing and subsequently classifying this activity continues to be a problem. When questioned about yearly reports of hacker attacks against the DOD, several key DOD and government subject matter experts provided the following responses:

- Air Force Maj. General John Campbell, commander of the Joint Task force for Computer Network Defense said the number of attacks was approximately 250,000, with unauthorized intrusions equaling 22,144 in 1999. (Verton, 2000:10)

- Lt. General David Kelley, director of the Defense Information Systems Agency said unauthorized intrusions increased about 300 percent, 5,844 in 1998 to 18,433 in 1999. (Ibid.:10)

- Lt. Col. LeRoy Lungren, program manager for the Army's National Security Improvement Program, said the Army had 285,000 network queries in 2000. (Ibid.:10)

- The Department of Justice said the number of government hacking cases increased from 547 in 1998 to 1,154 in 2000. (Ibid.:10)

Not only were the figures stating the magnitude of the problem different, but also with respect to this study, these subject matter experts used different words to describe the problem. This is not solely their fault.

By looking at the Air Force's Internet security information collection process, one can see that the process itself adds to the ambiguity. Appendix E and Appendix F contains examples of the forms the Air Force Computer Emergency Response Team

(AFCERT) uses to gather Internet security incident from the Air Force community.

AFCERT provides "information protect (IP) assistance to Air Force units" (AFCERT,

2000). These forms allow Air Force personnel to report Internet security activity

information to the AFCERT. AFCERT's peers, the Army CERT (ACERT), the CERT

Coordination Center (CERT®/CC), the DOD CERT, the Federal Computer Incident

Response Center (FeDCIRC), and the Navy Computer Incident Response Team

(NAVCIRT) use similar forms to collect Internet security activity information. Appendix G

through Appendix L contains examples of their forms.

Table 3 provides further examples detailing the problem of classify Internet

security attacks and incidents. Table 3 lists keywords from various sources

encompassing communication, computer, network, and Internet security used to

describe Internet security attacks and incidents.

Table 3 - Internet Security Attacks and Incidents Keyword List

Howard's 1997 Study	2000 Information Survey	AFDIR 33-303	AFSSI 5021
• Access attempts • Account break-in • Corruption of information incidents • Denial-of-service • Disclosure of information incidents • Root break-in	• Attacks on bugs in Web servers (e.g., CGI script-related attacks) • Attacks related to insecure passwords • Attacks related to protocol weaknesses • Buffer overflows • Denial-of-Service • Exploits related to active program scripting/mobile code (ActiveX, Java, JavaScript, VBS • Viruses/Trojans/Worms	• Compromise • Computer Crime • Computer Security Incident • Impersonation (a form of spoofing) • Malicious Logic/Virus/Worm • Vulnerability	• Administrative Vulnerability • Breach • Incident • Intruder • Malicious Logic • Penetration • Technical Vulnerability
(Howard, *Analysis*, 1997:93)	(Briney, 2000:40)	(Department of the Air Force, *AFDIR 33-303*, 1999)	(Department of the Air Force, *AFSSI 5021*, 1996:8)

The keyword list contains similar terms used to describe Internet security incidents,

however a one-to-one correlation does not exist. In fact, the 2000 Information Survey

even uses two types of subcategories, insider and outsider. Thus, the confusing

answers given by the DOD and government subject matter experts appear to be

understandable. Consequently, the need to develop a coherent, consistent method to classify Internet security attacks and incidents exists.

The Research Questions

This thesis examines the computer and network attack taxonomies developed by Howard. Howard developed the taxonomies to help him classify Internet security incidents as part of his doctoral research and to develop a common language for computer security as part of a follow-on study. A resulting recommendation included continued evaluation of the computer and network attack taxonomy to make practical modifications. According to Howard, "the taxonomy developed for this research was found to be satisfactory" (Howard, *Analysis*, 1997:235). When interviewed about the review process of the taxonomy, Howard replied, "my dissertation taxonomy was only reviewed by the committee, although Tom Longstaff was both on my committee and one of the CERT managers" (Howard, *Interview*, 2000). Therefore, one research question for this study is, "Are Howard's 1997 and 1998 computer and network attack taxonomies still satisfactory?".

A second research question is, "How do the taxonomies compare to the information being collected about computer and network attacks?". Several civilian, government and military organizations collect information concerning computer and network attacks. If the taxonomies are satisfactory, making sure these organizations collect the appropriate information to use with them would help the taxonomies become accepted, and eventually used.

III. Methodology

I may not have gone where I intended to go, but I think I have ended up where I intended to be. Douglas Adams (qtd. in Quoteland.com, 2000)

Research Design

The study uses a qualitative research method to conduct this study, using two techniques: a questionnaire and content analysis. According to Dooley, qualitative research refers to "social research based on field observations analyzed without statistics" (Dooley, 1995:259). He succinctly described the analysis this researcher plans to perform:

> The analysis of qualitative data begins with the first observation. As the observation phase winds down, analysis becomes more intense. Analysis organizes the hundreds of pages of raw notes into a meaningful pattern. It interconnects discrete observations and locates these connected events within a small number of conceptual categories. As with a jigsaw puzzle, the researcher fits and refits the pieces according to a variety of tentative models until few unconnected pieces remain and the fit seems subjectively and logically satisfying.
>
> A final report gives the resulting "jigsaw" picture as clearly and convincingly as possible. A common reporting method combines quotations from interview with anecdotes from the field observations to illustrate and support the analyst's general arguments. In support of a casual model, the analyst may report the approximate frequency and distribution of the different categories of observations (for example, high versus low proselytizing) as evidence. Such event counts may even support basic statistical analysis, but the qualitative researcher seldom relies as heavily on statistics as does the quantitative researcher. (Dooley, 1995:271)

Based on the results of this process, this researcher will make inferences relative to the research question.

Methodology

Since this study includes both of Howard's taxonomies, the following methodology applies to both. Round 1 involves the 1997 computer and network attack

taxonomy and Round 2 involves the 1998 computer and network attack taxonomy. First, the researcher plans to analyze the computer and network attack taxonomy by using a questionnaire with Likert-style scaling. Likert-style scaling "consists of a statement followed by a number of possible levels of agreement (for example, from 'strongly agree' to 'strongly disagree')" (Dooley, 1995:103). This researcher selected a 4-point scale to compel the respondents to make a discrete decision about the taxonomy, thereby reducing the possibility of the researcher misinterpreting the respondents' level of agreement with the questions. The questions came from Howard's definition and characterization of a satisfactory taxonomy. Thus, the respondents will base their professional judgments using the same criteria as Howard.

This researcher plans to use a nonprobability sampling method to select respondents to complete the questionnaire. Nonprobability sampling is "any method in which the elements have unequal chances of being selected" (Dooley, 1995:135). As a result, this researcher will use a purposive sampling procedure to select the elements, which are the respondents. In purposive sampling, the researcher "chooses respondents because of certain characteristics" (Ibid.:136). This researcher will select respondents based upon characteristics related to their background and knowledge, not their job category or job description. This differentiation is necessary because information security functions and responsibilities span several disciplines, as illustrated in the Information Magazine 2000 Information Security Survey in Table 4. In addition, these security professionals allocate various portions of their job responsibilities to their job of information security as illustrated in Table 4.

Table 4 - Job Category

Job Category	Percentage
Unit/Department/Division Manager	20%
Consultant	15%
CISO	14%
Engineer/Developer	14%
Administrator/Operator	12%
Analyst	11%
Executive/Partner/Principal	9%
Auditor	5%
	100%

(Briney, 2000:42)

Table 5 - Portion of Job Responsibilities Devoted to Infosecurity

Portion of job responsibilites devoted to infosecurity	Percentage
Part	59%
All	40%
None	1%
	100%

(Briney, 2000:42)

The significance of this information is that "a Forrester Research survey conducted this past May found that only about half of managers participate in risk management activities. To a certain extent, that suggests that security is riding the coattails of business initiatives that involve security, but aren't necessarily security-driven" (Briney, 2000:44).

Therefore, knowledge, not job category or job position is more important for this analysis, thus the purposive sampling technique. With that in mind, the characteristics used to select the respondents for this study were Air Force military member, Air Force civilian professional, or civilian professional with a background in the following disciplines: computer security, information security, communication security, information assurance, Internet security, and information warfare.

Although the respondents represent a larger population, this researcher will not use their responses or generate statistics intended to generalize to the larger population. Their responses, based upon their professional opinions, will only be used to analyze if the taxonomies are still satisfactory within the constraints of this study. In addition, the questionnaire represents categorical data, not numerical data. Consequently, they represent "arbitrarily selected numerical codes for the categories and have no utility beyond that" (McClave, Benson, and Sincich, 1998:14). However, the data can be ranked and meaningfully ordered, which this researcher plans to do. This data will be used to infer the level of agreement the respondents have with Howard's description of satisfactory.

Next, this researcher will perform a content analysis of the comments submitted by the respondents and the business forms used by Internet security activity organizations. Content analysis "is a research technique for making replicable and valid inferences from data to their content" (Krippendorff, 1980:21). This researcher will use the analytical semantics textual analysis approach. According to Rosengren, "it is possible to make reasonable interpretations of a text. The reasonableness is dependent on certain contextual claims, which can be linguistical, logical, semantical, or empirical" (Rosengren, 1981:29).

With respect to the questionnaire, this researcher will use the comments submitted by the respondents for any Disagree or Strongly Disagree selection, as well as the comments submitted for question 7. Question 7 explicitly solicits inputs for areas of improvement for the taxonomy. Both sets of comments use an open-ended question format. Open-ended questions are, "questions in interviews and on questionnaires that have no pre-specified answers" (Hoffer, George, and Valacich, 1998:244). In addition, each respondent is encouraged to "talk about whatever interests him or her in within the

general bounds of the question" (Ibid.:244). Upon completion of the content analysis of

the respondents' comments, the researcher will analyze the business forms used by

Internet security organizations to collect information on Internet security activity.

According to Hoffer, George, and Valacich, "[...] a document useful to systems

analysts is a business form [...]" (1998:255) because "forms are important for

understanding a system because they explicitly indicate what data flow in or out of a

system [...]" (Ibid.:257). Consequently, this researcher will analyze the business forms

used by various Internet security activity organizations, to determine if these

organizations collect appropriate information which will help Internet security

professional adequately use the computer and network taxonomy to classify Internet

attacks and incidents. These organizations are:

a. Army Computer Emergency Response Team (ACERT)
b. Air Force Computer Emergency Response Team (AFCERT)
c. Computer Emergency Response Team Coordination Center (CERT®/CC)
d. DOD Computer Emergency Response Team (DOD CERT)
e. Federal Computer Incident Response Center (FeDCIRC)
f. Navy Computer Incident Response Team (NAVCIRT), this includes the Marine Corps

Similar to the rationale for selecting the questionnaire respondents, the researcher

selected these organizations because they represent a collective community of similar

interest. This researcher also included the CERT®/CC because it was Howard's data

source for his study and because it is the de facto Internet security community leader, as

stated in the 1988 DARPA press release:

> In providing direct service to the Internet community, the CERT will focus on the special needs of the research community and serve as a prototype for similar operations in other computer communities [...].
>
> It will also serve as a focal point for the research community for identification and repair of security vulnerabilities, informal assessment of existing systems in the research community, improvement to emergency response capability, and user security awareness. (CERT®/CC, *DARPA*, 2001)

This researcher will develop a process-to-data entity matrix, illustrated in Table 6 and Table 7 as output from this analysis. A process-to-data entity matrix "identifies which data are captured, used, updated, or deleted within a process" (Hoffer, George, and Valacich, 1998:174). This process-to-data entity matrix will provide a more detailed view of the correlation between the information collected by these Internet security organizations and the computer and network attack taxonomies.

Table 6 - Business Form vs. 1997 Taxonomy Categories Matrix Example

	ATTACKERS	TOOLS	ACCESS	RESULTS	OBJECTIVES
ACERT					
AFCERT					
CERT®/CC					
DOD CERT					
FeDCIRC					
NAVCIRT					

Table 7 - Business Form vs. 1998 Taxonomy Categories Matrix Example

	ATTACKERS	TOOLS	VULNERABILITY	ACTION	TARGET	UNAUTHORIZED RESULT	OBJECTIVES
ACERT							
AFCERT							
CERT®/CC							
DOD CERT							
FeDCIRC							
NAVCIRT							

IV. Results and Analysis

There is one thing even more vital to science than intelligent methods; and that is, the sincere desire to find out the truth, whatever it may be." Charles Sanders Pierce (qtd. in Quoteland.com, 2000)

Round 1 - 1997 Computer and Network Attack Questionnaire

This researcher developed a questionnaire, contained in Appendix A, to analyze the level of agreement that the respondents had that the computer and network attack taxonomy was satisfactory. The questionnaire provided a mechanism to gather information concerning the taxonomy in a consistent manner, from all respondents. This researcher calculated composite scores for each question by summing up the scores of each item, in this case the level of agreement selected, for each question (Dooley, 1995, 103). Each question carried the same weight, meaning each question was considered just as important as the other, for the purposes of this study. In addition, Howard stated that his committee, which consisted of four members, reviewed his taxonomy and found it to be satisfactory. This researcher released 18 questionnaires and received 10 back, resulting in a 56% response rate. The number of returned questionnaires, each representing a single respondent, surpassed the total number of reviewers for Howard's original study; this was a goal of this process.

Overall, the majority of the respondents agreed that the 1997 computer and network attack taxonomy was satisfactory. The modal level of agreement for questions 1 – 6, which is also the item receiving the highest composite score for each question, was Agree. Underscoring this modal level of agreement by the respondents was the fact that one hundred percent of the respondents selected Agree for question 6, the only question to receive a unanimous opinion. Question 6 explicitly asks the respondents

42

about their level of agreement with the statement that the taxonomy is useful. No respondent selected either extreme level, Strongly Agree or Strongly Disagree. Table 8 lists the composite scores for questions 1 – 6 of the questionnaire.

Table 8 - Composite Scores of 1997 Taxonomy Questionnaire

Question	Strongly Agree	Agree	Disagree	Strongly Disagree
1. The computer and network attack taxonomy meets the described characteristics of **MUTUALLY EXCLUSIVE**.	0	6	4	0
2. The computer and network attack taxonomy meets the described characteristics of **EXHAUSTIVE**.	0	6	4	0
3. The computer and network attack taxonomy meets the described characteristics of **UNAMBIGUOUS**.	0	6	4	0
4. The computer and network attack taxonomy meets the described characteristics of **REPEATABLE**.	0	6	3	0
5. The computer and network attack taxonomy meets the described characteristics of **ACCEPTED**.	0	8	1	0
6. The computer and network attack taxonomy meets the described characteristics of **USEFUL**.	0	10	0	0

Although the modal level of agreement for questions 1 – 6 was Agree, those respondents that selected Disagree provided valuable information concerning the taxonomy. The following paragraphs summarize their comments. Appendix B, Table 12 contains all the respondents' comments, verbatim.

Question 1 inquired about mutual exhaustiveness. The respondents felt that although Howard defined discrete categories, the respondents provided several examples of the existence of overlap between categories. The statement about a hacker can wear two hats, one as a terrorist working for an enemy nation and one as a vandal causing frivolous damage, was a clear example. They also pointed out that

43

overlap can, and mostly likely does, exist between every category. One interesting observation is that the respondents focused primarily on the Attacker category.

Question 2 inquired about exhaustiveness. Since several respondents were Air Force members, this question resulted in a few military specific comments. Internet incidents for military purposes did not appear to be included in the taxonomy, according to some respondents, although one can speculate that a terrorist working for a nation/state under military control would qualify as a military operation classification. Additionally, Howard's list of tools does not include energy pulses or the tried and true social engineering. As such, the respondents do offer clear examples that the taxonomy may not be as exhaustive as it seemed initially.

Question 3 inquired about unambiguousness. These comments appear to be closely related to the mutual exclusivity comments. If issues exist with mutual exclusivity, then it is not surprising that issues also exist with unambiguousness. As stated, the objective of an incident may be to obtain some type of monetary payoff, however that payoff action may have resulted from the theft of valuable information. Therefore, how would one classify this event? As illustrated earlier in the use of various terms to describe Internet security incidents, clearly and concisely defining these actions continues to be a problem.

Question 4 inquired about repeatability. The comments provided appear to question the repeatability characteristic of the taxonomy. First, if issues exist with mutual exclusivity and unambiguousness, then how can one repeat the classification process the same way, if one is confused about which category to use? Second, based on the issues stated, how can the taxonomy appear logical if issues exist? The answer may be in logic itself. If one uses logic, or more appropriately, common sense reasoning, then it is likely that the process of classifying incidents could be repeated.

However, this appears to defy the purpose of a taxonomy. By definition, a taxonomy is a "division into ordered groups or categories" ("Taxonomy"). Therefore, one would simply classify, or place, an incident in the appropriate group or category, with little to no reasoning required. It is worth noting that in Howard's discussion on developing the computer and network attack taxonomy, repeatability appeared to be a problem with several of the taxonomies discussed.

Question 5 inquired about acceptability. Although one respondent disagreed with this question, the disagreement appears to be with the term Accepted. Howard defined accepted as, "logical and intuitive so that they could become generally approved" (Howard, Analysis, 1997:53). Since the modal level of agreement for this question was Agree, it appears the majority of respondents understood the taxonomy and believed it was logical and intuitive.

Question 6 inquired about usefulness. As stated earlier, this was the only question that all the respondents came to the same conclusion, by selecting Agree. Even with the questions about the other classification categories, all the respondents, to include those who disagreed about other areas, selected Agree. Unfortunately, no additional comments were provided, so this researcher would have to speculate about this result. Notwithstanding the lack of comments, the cliché, a picture is worth a thousand words, could justly apply. As noted in this study, and others, identification, classification, and even annotation of Internet security incidents are a problem. As Howard noted:

> The Internet is a scary place. At least that's what we've been told by numerous authors -- scholars and sensationalists alike [...]. Prior to this research, our knowledge of security problems on the Internet was incomplete and primarily anecdotal. Despite our increasing reliance on the computer networks, there had been no systematic and coordinated program for gathering and distributing information about Internet security incidents. (Howard, *Analysis*, 1997: 1)

As such, the fact that the computer and network attack taxonomy may be one of the first graphical descriptions of the intruder *process* viewed by the respondents, the taxonomy itself could be the reason behind the unanimous selection of Agree for question 6.

Finally, question 7 was an unadulterated solicitation for suggestions for areas of improvement to the taxonomy. This solicitation in no means suggests that Howard's work is flawed. In contrast, it is recognition of the process that Howard developed. According to Hammer and Champy, a process is "a collection of activities that takes one or more kinds of inputs and creates an output that is of value to a customer" (Hammer and Champy, 1993:35). In this case, Howard created a process to assist the Internet security professionals by taking their inputs, a security anomaly, and turning it into something useful, a classified attack or incident. In fact, the taxonomy is a process itself, starting with the attacker's perspective and ending with the attacker's objectives (Howard, *Analysis*, 1997:71). Therefore, change should be considered a normal part of the life of any process, not an indication of a flaw.

The respondents provided numerous recommendations on areas of improvement to the taxonomy, which are listed in Appendix B, Table 13. Several trends and ideas resulted from the information provided by the respondents. It is interesting to note that many of the suggestions appear as items lacking in the taxonomy, in actuality they reflect two issues underlying this study: lack of a common language and lack of a structured method to classify Internet security incidents. As noted by Howard and Longstaff, "much of the computer security information regularly gathered and disseminated by individuals and organizations cannot currently be combined or compared because a 'common language' has yet to emerge in the field of computer security" (Howard and Longstaff, 1998:iii). As such, what may appear as something

missing may in fact exist, however it is referenced differently. In addition, since a structured process does not appear to exist, it is possible that the respondents' interpretation of the taxonomy process differs.

Howard also noted that, "it should be expected, however, for a satisfactory taxonomy to be limited in some of these characteristics. A taxonomy is an approximation of reality that is used to gain greater understanding in a field of study. Because it is an approximation, it will fall short in some characteristics" (Howard, *Analysis*, 1997:53). Notwithstanding these issues, several threads appeared after analyzing the suggestions from the respondents.

In general, as indicated by several comments from the respondents, questions exist about the completeness of the classification categories, mutually exclusive, exhaustive, unambiguousness, repeatable, accepted, and useful. Howard published the taxonomy in 1997, however as stated in this study, the Internet and peripheral industries have experienced tremendous growth and change since then. As such, it makes sense that the taxonomy may not reflect the current language used today, with respect to Internet security activity.

Concerning the Attacker category, the taxonomy does list several types of Attackers, but some respondents felt it needs to differentiate between insider and outsider. An insider refers to "full- or part-time employees, contracted workers, consultants, company partners or suppliers" (Briney, 2000:48) and outsider refers to "everyone not included in the description for 'insider'" (Ibid.:49). This differentiation could apply to all the Attacker types included in the taxonomy. In addition, several comments had a military slant to them, such as information warfare and the observe, orient, decide, and act (OODA) Loop. As noted, several respondents were Air Force officers, who obviously have a military view to many things.

Several key issues resulted from the comments on the Tools category. First, the Tools category implies, or leads one to interpret, that each tool listed refers to a single process. To clarify, a respondent annotated that Attackers most likely use one or more tools to accomplish their goal, and the taxonomy requires the user to chose a specific tool. This leads into the second key issue, interpretation of the taxonomy. Again, one respondent noted that one may interpret that all the blocks on the taxonomy line up horizontally, therefore, hackers goes to user commands which goes to implementation vulnerability, etc. As stated earlier, interpretation of the taxonomy itself many lead one to assume it is lacking in certain areas. Finally, some respondents felt the Tools category focused solely on the technical aspects of Internet security activity. Based on one's interpretation of Tools, this category does not include Social Engineering, stealing of passwords, and simple human error as tools towards obtaining the objective.

The Access category appears to contain three distinct groupings of information. It was the only category that a respondent clearly stated that the meaning of this category was unclear. However, similar to the Tools comments, issues such as Social Engineering, stealing of passwords, and simple human error appear to be missing. Although, one can argue that problems with implementation, design, configuration, and access control can result from human error.

The Results category comments followed the same trend as the other categories. Even though Howard wanted to avoid simply listing items, lists to occur within each category. As such, lists tend to leave one opened to the question, "Why didn't you include this one?" The respondents offered several other types of Results, to include financial loss, customer goodwill loss, posturing for future actions, and permanent destruction of information. An interesting comment concerned the issue that the taxonomy appears to focus on short-term, not long-term results. The respondent

suggested that an Attacker's objective might take a long time to achieve. This end to the means may result in several of the categories listed by Howard, in both the short-term and the long-term, as the Attacker works towards the end objective; this is a very interesting concept. Consequently, the respondent appears to believe that the taxonomy misses this concept, and implies that a Result is the end of the Attacker's work, which immediately leads to an Objective.

Finally, the Objectives category comments also resemble those previously stated. The listing itself causes one to question why something was not included. The respondents suggested items such as distinguishing between personal and corporate gains and including the military perspective. However, one can argue that the entertainment and education objectives are not missing, but are included within the challenge and status list.

Even with all the suggested areas of improvement, the most important information obtained from the questionnaire was that the respondents agreed that the taxonomy was satisfactory. The fact that the modal level of agreement for questions 1 – 6 was Agree and that all the respondents selected Agree for the question that explicitly asked them do they agree with the statement that the taxonomy meets the characteristics described as useful, supports this claim.

Round 1 - Internet Security Information Collected verses the 1997 Taxonomy

This researcher found that although many organizations collect information on Internet security activity, they do not freely release this information. Due to national security concerns by the DOD and liability concerns of the private sector, these organizations maintain strict security and confidentiality policies to protect the information. Consequently, how can one operationally test the computer and network

taxonomy? The method used by this researcher involved content analysis of the business forms used by these organizations to collection Internet security activity information. By analyzing these business forms, one can determine if the information being collected is appropriate to use as inputs into the computer and network attack taxonomy. In other words, are these organizations collecting the appropriate information, which will help Internet security professionals adequately use the computer and network taxonomy to classify Internet attacks and incidents?

This researcher collected and analyzed the business forms used by the following Internet security organizations:

a. Army Computer Emergency Response Team (ACERT)
b. Air Force Computer Emergency Response Team (AFCERT)
c. Computer Emergency Response Team Coordination Center (CERT®/CC)
d. DOD Computer Emergency Response Team (DOD CERT)
e. Federal Computer Incident Response Center (FeDCIRC)
f. Navy Computer Incident Response Team (NAVCIRT), this includes the Marine Corps

These business forms, located in Appendix E through Appendix L, detail the information collected by these organizations to record Internet security activity. Table 9 illustrates the relationship between the Internet security organizations' business forms and the 1997 taxonomy. A "Y indicates that the organization explicitly requests information relative to that specific category. An "N" indicates that the organization does not explicitly request information relative to that specific category.

Table 9 - Business Form vs. 1997 Taxonomy Matrix

	ATTACKERS	TOOLS	ACCESS	RESULTS	OBJECTIVES
ACERT	N	Y	Y	Y	N
AFCERT	N	Y	Y	Y	N
CERT®/CC	N	Y	Y	Y	N
DOD CERT	N	Y	Y	Y	Y
FeDCIRC	N	Y	Y	Y	N
NAVCIRT	N	Y	Y	Y	N

As illustrated above, all the organizations explicitly request information relative to the Attackers, Tools, Access, and Results categories. The organizations have data entry fields either specifically labeled using the same words as the taxonomy category or very similar words. For example, the NAVCIRT form contains the data entry item, "9. Damage or effects resulting from attack" (Department of the Navy, 1998). The only organization that appears to explicitly request information about the Objectives was the DOD CERT, otherwise none of the business forms contained any explicit reference to Attackers or Objectives. In fact, this researcher only assumes that it is possible that some victims include this type of information via the catchall data entry field, usually labeled Describe the Incident.

Additional information gleaned from analyzing the business forms included the finding that no standard form existed. Although the organizations use similar data entry fields, a single form did not exist. A standard form would help the reporting process and the information sharing process. Next, all the organizations provide the catch all data entry field, Describe the Incident. The necessity of this data entry is obvious, however the information entered is usually written from the victim's perspective, which most likely

is different for each victim. The most interesting thing concerning this data entry field, is the fact that the CERT®/CC appears to depend solely on this data entry field as its source of information. The CERT®/CC's business form was the weakest, or less specific, of all. This is surprising because it is assumed the CERT®/CC, which is the de facto leader of the CERTs, collects the most detailed information of all. Finally, the ACERT and AFCERT use two forms to collect their information; one form to report intrusions or incidents, and one form to report malicious code. Although both are distinct events, the need for two forms is unclear, especially since the NAVCIRT explicitly collects both types of information on one form.

Although the Internet security activity monitoring organizations explicitly collect information that can be used as input into the computer and network attack taxonomy, they do not explicitly collect all the necessary information. As a result, there maybe a disconnect between the information collected and the information needed by the taxonomy.

Round 2 - 1998 Computer and Network Attack Questionnaire

This researcher developed a questionnaire, contained in Appendix C, to analyze the level of agreement that the respondents had with the 1998 computer and network attack taxonomy was satisfactory. The researcher followed the same methodology used for the 1997 taxonomy questionnaire. This researcher released 10 questionnaires to the respondents that **replied** to the 1997 questionnaire, and received 7 back, resulting in a 70% response rate.

Overall, the majority of the respondents agreed that the 1998 computer and network attack taxonomy was satisfactory. The modal level of agreement for questions 1, 3, 4, 5, and was Agree, and the modal level of agreement for question 2 was Strongly

Agree and Agree. In fact, each question received at least one Strongly Agree selection. No respondent selected the other extreme level of agreement, Strongly Disagree. Table 10 lists the composite scores for questions 1 – 6 of the questionnaire.

Table 10 - Composite Scores of 1998 Taxonomy Questionnaire

Question	Strongly Agree	Agree	Disagree	Strongly Disagree
1. The computer and network attack taxonomy meets the described characteristics of **MUTUALLY EXCLUSIVE.**	1	<u>4</u>	2	0
2. The computer and network attack taxonomy meets the described characteristics of **EXHAUSTIVE.**	<u>3</u>	<u>3</u>	1	0
3. The computer and network attack taxonomy meets the described characteristics of **UNAMBIGUOUS.**	2	<u>4</u>	1	0
4. The computer and network attack taxonomy meets the described characteristics of **REPEATABLE.**	2	<u>4</u>	1	0
5. The computer and network attack taxonomy meets the described characteristics of **ACCEPTED.**	2	<u>5</u>	0	0
6. The computer and network attack taxonomy meets the described characteristics of **USEFUL.**	3	<u>4</u>	0	0

Although the modal level of agreement for questions 1 – 6 was Agree, or Strongly Agree and Agree for question 2, those respondents that selected Disagree provided valuable information concerning the 1998 computer and network attack taxonomy. The following paragraphs summarize their comments. Appendix D, Table 14 contains all the respondents' comments, verbatim.

Question 1 inquired about mutual exclusiveness. A respondent believed that there needed to be a distinction between internal and external user attack, because the respondent believes internal users cause more damage. However, upon closer examination, the respondent may be referring to accidental damage caused by internal

users; this was not clear. In addition, another respondent reiterated the common theme that the category may not be mutually exclusive, or in other words, as complete as possible. Again, lists of items almost inevitably leave something out.

The remaining questions, which inquired about exhaustiveness, unambiguousness, repeatability, acceptability, and usefulness, resulted in two total comments. The comments simply question the completeness of the categories and the interpretation of the taxonomy. Once again, claiming that a category contains everything appears to challenge one to find the missing piece. In addition, individual interpretation of the taxonomy may lead to problems with ambiguousness and repeatability. The respondents submitted no comments about acceptability and usefulness.

The respondents provided several recommendations on areas of improvement to the 1998 computer and network attack taxonomy, which are listed in Appendix D Table 15. Two trends appeared after analyzing the comments. First, the respondents appeared to approve of the 1998 version of the taxonomy over the 1997. Their comments include words such as much better, good, and no changes. Second, questions over the completeness and interpretation of the taxonomy were apparent. To reiterate, Howard published this taxonomy in 1998, which was static, compared to the Internet, computers, and networks, which are dynamic.

Concerning the Attacker category, the respondents believed Howard's construct was not only better than his 1997 taxonomy, but it appeared to represent Attackers in a more acceptable way. The respondents appeared very pleased with the description of this category. However, they did offer more suggestions on the continued stratification of the category, such as distinguishing between hackers and crackers. Finally, a comment that applies to the taxonomy in general is that one's interpretation of the taxonomy may affect what is determined as missing or not missing.

The comments about Tools appeared to be more questions about Howard's definition of Tools, than anything else. Working in such a dynamic profession, many accepted definitions, words, and phrases change frequently. However, by the nature of the comments, they may implicitly justify the necessity of the computer and network attack taxonomy to ensure everyone speaks the same language. Also, a respondent provided an excellent example about why the questions exist about completeness of the taxonomy, specifically mutual exclusiveness and unambiguousness. Toolkits, a tool, consists of tools. How should these be classified? Therefore, one respondent believed an obvious overlap exists with Toolkits and the tool types listed in the taxonomy.

Vulnerability received an interesting comment about the focus of the taxonomy. Although Howard designed that the taxonomy from the attacker's perspective, a respondent felt it focused more on the technological side of the issue. The respondent clearly emphasized that the human element plays a role. The best security technology cannot account for all human mistakes. Therefore, the respondent may be implying that this category, and probably others, needs to reflect more of the human element within this process.

The next categories, Action, Target, Unauthorized Result, and Objectives received few comments. The comments provided simply acknowledged the respondents' belief that the categories appropriately captured the content, or reiterated questions about the taxonomy's completeness. The respondents appeared to understand the meaning of Action, Target, Unauthorized Result, and Objectives. Those who did not stated that one's interpretation of the taxonomy might result in different meanings.

The respondents appeared to have a high level of agreement with Howard's 1998 computer and network attack taxonomy. Not only did some respondents select

Agree, some also selected Strongly Agree as their selection for a question. In fact, question 2, which inquired about exhaustiveness, resulted in Strongly Agree and Agree receiving the same composite score. In addition, the comments included questions about the taxonomy's completeness and suggested further levels of details, however the comments also included accolades toward the 1998 taxonomy.

Round 2 - Internet Security Information Collected verses the 1998 Taxonomy

The organizations that collect Internet security activity information explicitly collect some, but not all information necessary for inputs into the taxonomy. Table 11 illustrates the relationship between the Internet security organizations' business forms and the 1998 computer and network attack taxonomy. A "Y indicates that the organization explicitly requests information relative to that specific category. An "N" indicates that the organization does not explicitly request information relative to that specific category.

Table 11 - Business Form vs. 1998 Taxonomy Matrix

	ATTACKERS	TOOLS	VULNERABILITY	ACTION	TARGET	UNAUTHORIZED RESULT	OBJECTIVES
ACERT	N	Y	N	Y	Y	Y	N
AFCERT	N	Y	N	Y	Y	Y	N
CERT®/CC	N	Y	N	Y	N	Y	N
DOD CERT	N	Y	N	Y	Y	Y	Y
FeDCIRC	N	Y	N	Y	Y	Y	N
NAVCIRT	N	Y	Y	Y	Y	Y	N

This process-to-data entity matrix also indicates that as the level of detail gets finer, it appears the Internet security organizations need to ask more direct questions to obtain the necessary information to use the 1998 taxonomy. The business forms used by the Internet security organizations appear to request less detailed information than what the 1998 taxonomy requires. As stated earlier, the de facto CERT leader

CERT®/CC appears to collect less detailed information than all the other CERTs.

Regardless, these organizations do collect some information useful to the taxonomy and

with some work and coordination with the taxonomy developers, they can most likely

explicitly collect more.

V. Discussion and Conclusion

When you make the finding yourself - even if you're the last person on Earth to see the light - you'll never forget it. Carl Sagan (qtd. in Quoteland.com, 2000)

Discussion

Based on the results of the 1997 and 1998 computer and network attack taxonomy questionnaires, this researcher concludes that Howard's taxonomies are satisfactory. Overall, the majority of the respondents agreed that the 1997 taxonomy was satisfactory because the modal level of agreement for questions 1 – 6 was **Agree**. Underscoring this fact was that one hundred percent of the respondents selected **Agree** for question 6, which explicitly asks the respondents about the statement that the taxonomy is useful. In addition, the majority of respondents agreed that the 1998 taxonomy because the modal level of agreement for questions 1, 3, 4, 5, and was **Agree**, and the modal level of agreement for question 2 was **Strongly Agree** and **Agree**. In fact, questions 1 – 6 all received at least one Strongly Agree selection.

It appears that the respondents preferred the 1998 taxonomy over the 1997 taxonomy. First, the 1998 taxonomy received 13 Strongly Agree selections, while the 1997 taxonomy did not receive any. Second, the 1998 taxonomy received fewer areas of improvement comments than the 1997 taxonomy. Third, the 1998 taxonomy received several accolades on its contents, while the 1997 received none. It is important to note that the same group of respondents analyzed both taxonomies.

Although the respondents agreed that the taxonomies as a whole were satisfactory, they did find areas of improvement with them. They offered evidence that questioned the completeness of the taxonomy. In addition, they also indicated that even though the taxonomy may have met the definitions of mutually exclusive, exhaustive,

unambiguous, repeatable, accepted, and useful, these categories may still need work to persuade others to fully agree with the statements. However, the transition from the 1997 taxonomy to the 1998 taxonomy appeared to have addressed many of the respondents' concerns. The additional stratification of the taxonomy appears to have provided the level of detail that the respondents agreed with.

With respect to the relationship of the Internet security organizations' information gathering process and the taxonomy, there appears to be a disconnect. These organizations do explicitly collect some, but not all, the information necessary as inputs into the taxonomies. The analysis of both taxonomies resulted in similar findings, except that the 1998 taxonomy required more detailed information. Since the computer and network attack taxonomy is relatively new, it is quite likely that these organizations either are not aware of the taxonomy, or if aware, have not accepted its use. Regardless, some of the necessary information is explicitly collected.

Along that line, explicit requests for information on Attackers and Objectives appeared lacking. First, several of the organizations requested the Internet Protocol (IP) address as a method to identify the source of the attack. The IP address is actually part of the Transmission Control Protocol/Internet Protocol (TCP/IP), which is the suite of protocols used to send and receive information across the Internet. By definition, TCP/IP is:

> The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams. (Department of the Air Force, 33-129, 1999:44)

On the surface, using the IP address to identify attackers seem reliable, however based on IP Spoofing, it is not. IP spoofing is:

> The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to "change his identity" and appear as a valid machine within the network. (Ibid.:43)

Therefore, requesting the IP address alone does not provide enough information to adequately, and confidently identify the Attackers.

Second, the lack of explicit requests for information relative to the attackers Objective appears to be more nebulous. As indicated in Table 9 and Table 11, the DOD CERT appears to be the only Internet security organization that explicitly requests information on the attackers' objective, via their **Why** field of their business form. It is unknown exactly what information goes into this field, however at least the DOD CERT asks the questions.

The analysis of the information collection process did reveal some interesting information. First, the information collection process appeared disjointed between the organizations. For example, they do not use standard forms to collect the Internet security activity information. As such, each organization asks different questions, from different perspectives, using different data entry methods, although they appear to be looking for the same thing; information on Internet security attacks and incidents. According to Hoffer, George, and Valacich:

> The goal of a form and report design is usability. Usability means that users can use a form or report quickly, accurately, and with high satisfaction. To be usable, designs must be consistent, efficient, self-explanatory, well-formatted, and flexible. (1998:540)

Obviously, the CERTs have business forms that allow them to collect information, however the inconsistencies noted indicate that a standard information collection

process does not exist. The lack of a standard data collection process appears to perpetuate the lack of a common language problem, by continuing to allow victims to report incidents in a somewhat haphazard fashion.

Limitations and Constraints

Although the respondents deemed the taxonomy satisfactory, it does have some limitations. First, it includes lists of items per category, which seems appropriate. However, as stated throughout this thesis, lists beg some to discover the missing piece, or at least what they perceive as the missing piece. Second, it appears to encapsulate the attacker's process well, however others do, as indicated by the respondents' comments, interpret the process differently. This may be a human characteristic, but it is important to note that not everyone interprets the process the same way. Finally, this study included observations and professional interpretations of the taxonomy. To further validate the model it needs to be operationally tested. Operational testing involves using actual incident reports to determine how effective the taxonomies in the classification of computer and network attacks and incidents. This testing will further validate the taxonomies and encourage its acceptance and use.

Concerning the respondents of the questionnaire, some limitations existed too. As indicated in Table 4, the information security profession traverses many disciplines. Although on one hand it can mean the information security level of awareness is high, since so many disciplines are concerned about it, but on the other hand, when specifically looking for the information security points of contact, it can be difficult. This researcher had to interview some of the respondents before allowing them to participate in the analysis, because it was not clear if they had the appropriate background. In more than one occasion, the original contacts responded by saying they were not the

appropriate persons for the interview, and referred the researcher to another contact. However, the sample size used for this study was small. A larger sample size should be used with future studies, which should allow the researcher to generalize to the larger population. Along that line, a comprehensive, validated survey instrument should be used to better capture the intent of the respondents.

Comprehensive information on Internet security incidents is lacking. According to Fred B. Schneider, Chair, Committee on Information Systems Trustworthiness, and editor of Trust in Cyberspace, "insufficient data exist about Internet outages and how the Internet's mechanisms are able to deal with them" (Schneider, et al., 1999:47). Schneider's committee participated in a DARPA and NSA requested study, in conjunction with the Computer Science and Telecommunications Board, the Commission on Physical Sciences, Mathematics, and Applications, and the National Research Council. The DARPA and NSA tasked the committee to "examine, discuss, and report on interrelated issues associated with the research, development, and commercialization of technologies for trustworthy systems and to use its assessment to develop recommendations for research to enhance information systems trustworthiness" (Schneider, et al., 1999:viii). Among other findings, the committee found that "a few university computer science departments have several faculty members who emphasize computer security research, but many departments have none who do. In any event, the number of computer security researchers is small compared to the number in other specialties [...]" (Ibid.:235). In short, the body of knowledge with respect to Internet security incidents is probably incomplete.

Of the available information, the lack of access to actual incident data was stifling to this researcher. For the purposes of this study, this researcher attempted to acquire Internet security information from the CERT®/CC, AFCERT, as well as the local

organizations. All denied access to their information due to security or confidentiality concerns. These concerns are valid, however if the Internet community, specifically researchers, cannot get access to this information, then how can the community learn to improve itself and its security methods?

Similarly, the lack of a standard business form to collect Internet security attack and incident information also limited this study. The use of different keywords and data entry formats required this researcher to literally figure out what the organizations were requesting. The forms were not consistent, self-explanatory, or well-formatted. Some were text documents converted into web pages, some were elaborate forms, and some were lists of several items to include in a report.

Implications for Researchers

The study revealed that the computer and network attack taxonomy appears to be on the right track to help the Internet security community effectively classify computer and network attacks and incidents. Future study of the taxonomy will help it mature and possibly become an accepted part of computer and network security profession.

In addition, this study also revealed that Howard's work towards developing a common language for computer security appears appropriate. As indicated, several of the computer emergency response teams do not use standard forms or standard language when requesting pertinent information. These organizations collect similar, but not totally the same type of information. Researchers should continue this path of examination to help the industry work towards a more coherent method of information collection and dissemination.

Implications for Practitioners

This study revealed that not only does Internet security appear to be a problem, but so is the process of describing the level of Internet security activity. Throughout this study *interpretation* appeared. American Heritage defines interpretation as, "the act of interpreting; explanation of what is obscure; translation; version; construction; as, the interpretation of a foreign language, of a dream, or of an enigma" ("Interpretation"). It is disconcerting that with issues such as national security, intellectual property rights, and electronic commerce at risk via the Internet that the industry continues to have difficulty plainly describing the status of Internet security. Practitioners should work towards a common model and common language to help the industry better address and identify risks associated these issues.

Recommendations for Future Research

Perhaps the most important recommendation is continued monitoring and examination of the computer and network taxonomy. This study revealed several areas of improvement of the taxonomy. These areas of improvement should be analyzed to determine their feasibility and to help validate the respondents' comments, as well as the second iteration of the computer and network taxonomy.

In addition to continued examination of the taxonomy, this researcher recommends operational testing of the taxonomy. Operational testing would allow one to use actual incident information to test the taxonomy, which moves forward from examining the concepts behind the taxonomy. Operational testing would further validate the taxonomy, as well as increase its exposure to, and possible acceptance by, the Internet security community.

To facilitate the use of the computer and network attack taxonomy, this researcher recommends development of a standard information collection process for Internet security activity. The development of a standard process would help all interested parties focus on the same kinds of information and probably lead to a common language too. In addition, this process could be coordinated with the maintainers of the computer and network taxonomy. This coordination would facilitate the taxonomy's use and acceptance by the Internet security community and ensure the information collection process collects the appropriate information necessary for the taxonomy.

By using prototyping and Rapid Application Development, which is a "systems development methodology created to radically decrease the time needed to design an implement information systems" (Hoffer, George, Valacich, 1998:835), that also benefits from "extensive user involvement" (Ibid.:835), a standard form can be developed, as shown in Appendix M, in a relatively quick fashion. The recommended standard form uses the common elements found on the business forms used by the CERTs analyzed for this study. Next, it includes all the distinct elements of Howard's 1998 taxonomy, because this version appeared to be the preferred version based on this study. By combining these two data sets, the CERTs can explicitly capture an abundance of information about computer and network attacks, plus the collected information would be appropriate as input into the computer and network attack taxonomy. In addition, the design of the form allows computer programmers to quickly convert the format into a functional database. Each line item on page 1 and each element on page 2 can map one-to-one to a database field, thus allowing the CERTs to better automate, analyze, and report on the status of Internet security activity. Finally, concerning flexibility for the uniqueness of the CERTs, each organization can add data elements as they deem

necessary. This allows the organizations to tailor the form to conform to any specific requirements they have. However, it is important that the standard sections of the form, in this case pages one and two, not be modified without total agreement from all the CERTs and the taxonomy developers. These sections represent the information that should be common across the board.

Finally, congruent to the development of a standard information collection process, an information release process should be developed. Taking into account the security and liability concerns, a process should be developed to help interested parties with valid reasons gain access to the collected data. Without access to this data, examining successes and areas of improvements will remain difficult.

Conclusion

This researcher concludes that Howard's 1997 and 1998 computer and network attack taxonomies are satisfactory, based upon the results of the questionnaires. The respondents did appear to agree with the 1998 taxonomy more than the 1997 taxonomy. It appears that the 1998 taxonomy appears to have addressed many of the areas of improvement comments submitted for the 1997 taxonomy.

In addition, this researcher concludes that there appears to be a disconnect between the organizations responsible for collecting Internet security data and the developers of the taxonomy. The organizations do collect some information that can be used as inputs to the taxonomy, but not all. If the taxonomies are to become accepted and used, then the data collectors and the taxonomy developers should coordinate their efforts.

Similarly, it appears that the organizations collecting information have not advanced past the early days of simply collecting an abundance of abstract information,
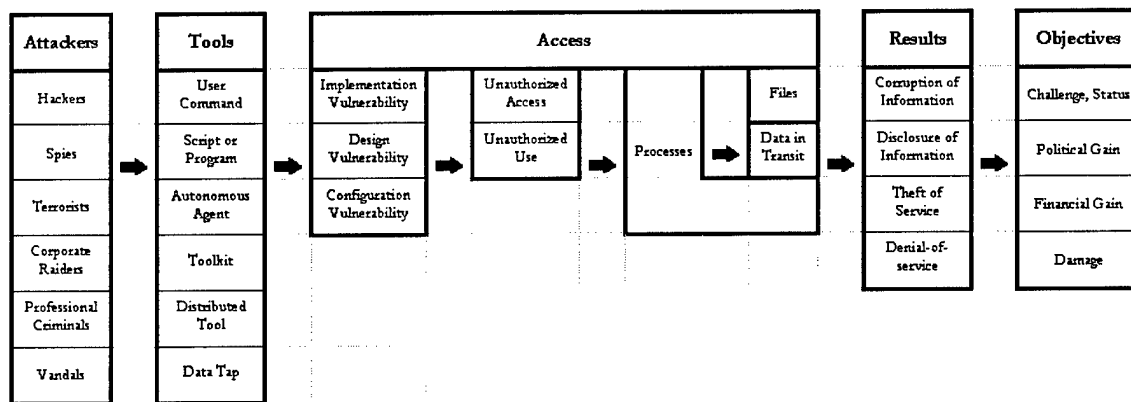
then trying to manually make sense of it all. Although this study indicated that problems still exist with distinguishing between different types of computer and network attacks and incidents, sufficient information technological resources exist to help these organizations collect and analyze this information better. Asking more direct questions of the victims to get the specifics, incorporating better database designs to store and retrieve the information, and using information technology as an enabler to help analyze this information would help move not only the information collection, but also the information dissemination process, move forward.

Along the same line of thought, this researcher concludes that a standard method for collecting computer and network attack information does not exist. The responsible organizations do not use a standard form to collect computer and network attack information, which results in each organization collecting similar, but not totally the same type of information. Without standardization, these organizations will continue to collect information concerning computer and network attacks and incidents in a haphazard fashion, which probably fuels the lack of a common language problem discussed in this study.

Finally, although the organizations gather information, this researcher concludes that without access to actual computer and network attack data, the ability to operationally test the taxonomies will continue to be difficult. The data collectors appear to be gathering valuable information about computer and network attacks. The computer and network attack taxonomy developers appear to have a model that some computer security professional agree with. Yet, obtaining the data to take the next testing step, operational testing, continues to be difficult. Operational testing will add to the validity of the model.

Appendix A - 1997 Computer and Network Taxonomy Questionnaire

This questionnaire supports the thesis, <u>An Analysis of the Computer and Network</u> <u>Attack Taxonomy</u>, written by Captain Richard C. Daigle, graduate student in the Information Resource Management degree program. Read the background information on Figure 1 – Computer and Network Attack Taxonomy and then proceed to the questionnaire. Your contributions will be used to analyze the **satisfactory** usefulness of the computer and network attack taxonomy, as defined by Mr. John D. Howard.

Attackers	Tools	Access						Results	Objectives
Hackers	User Command	Implementation Vulnerability	Unauthorized Access				Files	Corruption of Information	Challenge, Status
Spies	Script or Program	Design Vulnerability	Unauthorized Use		Processes		Data in Transit	Disclosure of Information	Political Gain
Terrorists	Autonomous Agent	Configuration Vulnerability						Theft of Service	Financial Gain
Corporate Raiders	Toolkit							Denial-of-service	Damage
Professional Criminals	Distributed Tool								
Vandals	Data Tap								

(Howard, *Analysis*, 1997: 73)
Figure 1 – Computer and Network Attack Taxonomy

Howard developed the computer and network attack taxonomy as part of his dissertation, <u>An Analysis of Security Incidents on the Internet 1989 – 1995</u>, which he submitted to Carnegie Mellon University, as part of his requirements for the Doctor of Philosophy degree in Engineering and Public Policy on 7 April 1997. The taxonomy was not peer reviewed or analyzed by anyone outside of himself and his committee. As such, the taxonomy does not represent an accepted model. However, it formed the basis for Howard's research and it has been referenced in at least two publications:

a. 1998 Sandia National Laboratories report, <u>A Common Language for</u> <u>Computer Security Incidents</u> by John D. Howard and Thomas A. Longstaff

b. 2000 Carnegie Mellon Software Engineering Institute Technical Report, <u>State</u> <u>of the Practice of Intrusion Detection Technologies</u> by Julia Allen, et al.

The following background information comes from a compilation of extracts from

Howard's research:

> This taxonomy depicts a simplification of the path an attacker must take in order to accomplish the attacker's objectives. To be successful, an attacker must find one or more paths that can be connected, perhaps simultaneously.

> Howard defined computer security as:

> > *Computer security* is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks. (Howard, *Analysis*, 1997:50)

> As the formal definition of computer security presented indicates computer security is preventing attackers from achieving objectives by making any complete connections through the steps depicted. More specifically, computer security efforts are aimed at the five blocks of the taxonomy.

> A popular and simple taxonomy of computer and network security attacks is a list of single, defined terms. Variations of this approach include lists of categories. There are several problems that limit the usefulness of these approaches including 1) the terms not being mutually exclusive, 2) an exhaustive list being difficult to develop and unmanageably long, 3) the definitions of individual terms being difficult to agree on, and 4) there being no structure to the categories.

> An alternate categorization method is to structure the categories into a matrix. The procedure for classification using these taxonomies, however, is not unambiguous when actual attacks are classified. In addition, the logic is not intuitive, and the classifications are limited in their usefulness.

> The taxonomy developed as part of this research does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather to reorient the focus of the taxonomy toward a process, rather than a single classification category.

> The final taxonomy presented was developed from the specific definition of computer security...from the criticisms of the current taxonomies, and from a process or operational viewpoint. From this viewpoint, an attacker on computers or networks attempts to link to ultimate objectives or motivations. This link is established through an operational sequence of tools, access, and results that connects these attackers to their objectives...

> The taxonomy "does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather attempts to provide a broad, inclusive framework. The intention was to reorient the focus of the taxonomy toward a process, rather than a single classification category, in order to provide

both an adequate classification scheme for Internet attacks, and also a taxonomy that would aid in thinking about computer and network security".

Extracted from An Analysis of Security Incidents on the Internet 1989 – 1995, by John D. Howard, http://www.cert.org/research/JHThesis/Start.html.

The following information further helps you understand the five categories of the computer and network attack taxonomy:

ATTACKERS

1. Attacker represents the people that attack computer and network services.

   a. Hackers - break into computers primarily for the challenge and status of obtaining access.
   b. Spies - break into computers primarily for information which can be used for political gain.
   c. Terrorists - break into computers primarily to cause fear which will aid in achieving political gain.
   d. Corporate Raiders - employees of one company break into computers of competitors for financial gain.
   e. Professional Criminals - break into computers for personal financial gain (not as a corporate raider).
   f. Vandals - break into computers primarily to cause damage.

TOOLS

2. Tools used to exploit computer and network vulnerabilities.

   a. User Command - the attacker enters commands at a command line or graphical user interface.
   b. Script or Program - scripts and programs initiated at the user interface to exploit vulnerabilities.
   c. Autonomous Agent - the attacker initiates a program, or program fragment, which operates independently from the user to exploit vulnerabilities.
   d. Toolkit - the attacker uses a software package which contains scripts, programs, or autonomous agents that exploit vulnerabilities.
   e. Distributed Tool - the attacker distributes tools to multiple hosts, which are then coordinated to perform an attack on the target host simultaneously after some time delay.
   f. Data Tap - where the electromagnetic radiation from a cable carrying network traffic, or from a host computer is "listened" to by a device external to the network or computer.

ACCESS

3. Access used to breach computer and network services.

    a. Vulnerability – a flaw that the attacker exploits to obtain unauthorized access or use of the computer and network services.

    b. Unauthorized access and use – Per Howard:

> Because I felt that it was more important to emphasize the *unauthorized* nature of an attacker's activities, I chose to use the first pair of terms (*unauthorized access* and *unauthorized use*), but it should be understood that *unauthorized use* implies *authorized access*. In addition, it should be understood that *unauthorized access* implies that this access will result in an *unauthorized use*. (Howard, *Analysis*, 1997:50)

> Both the means used to gain unauthorized access or use…as well as the ends of attacks…are included [in the computer security definition] because they require unauthorized access or unauthorized use. (Howard, *Analysis*, 1997:51)

    c. Processes, files and data in transit – protected resources which are the targets of the attackers, both individually and collectively.

RESULTS

4. Results of attack once the attackers obtains access to the protected resources and exploits the vulnerabilities.

    a. Corruption of Information - any unauthorized alteration of files stored on a host computer or data in transit across a network.

    b. Disclosure of Information - the dissemination of information to anyone who is not authorized to access that information.

    c. Theft of Service - the unauthorized use of computer or network services without degrading the service to other users.

    d. Denial-of-service - the intentional degradation or blocking of computer or network resources.

5. Objectives or primary motivations of the attackers gleaned from attacker categories.

    a. Challenge or Status – objective of hackers
    b. Political Gain – objective of spies and terrorists
    c. Financial Gain – objective of corporate raiders and professional criminals
    d. Damage – objective of vandals

According to Howard, a **satisfactory** taxonomy "should have classification categories with the following characteristics" (53):

1. Mutually exclusive - classifying in one category excludes all others because categories do not overlap
2. Exhaustive - taken together, the categories include all possibilities
3. Unambiguous - clear and precise so that classification is not uncertain, regardless of who is classifying
4. Repeatable - repeated applications result in the same classification, regardless of who is classifying
5. Accepted - logical and intuitive so that they could become generally approved
6. Useful - can be used to gain insight into the field of inquiry. (53)

Therefore, based upon the five category descriptions and the **satisfactory** taxonomy definition, please complete the following questionnaire to determine the degree that you agree with the assessment that the computer and network attack taxonomy is **satisfactory**. Since a taxonomy approximates reality, it may be limited in some of the characteristics.

Please answer the questions and short answers below. If you select **Disagree** or **Strongly Disagree** for questions 1 through 6, please provide an explanation.

- Date: _____

- Primary Air Force Specialty or corresponding job description (i.e. Communications-Computer Officer): _____

Question	Strongly Agree	Agree	Disagree	Strongly Disagree
1. The computer and network attack taxonomy meets the described characteristics of **MUTUALLY EXCLUSIVE.**	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
2. The computer and network attack taxonomy meets the described characteristics of **EXHAUSTIVE.**	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
3. The computer and network attack taxonomy meets the described characteristics of **UNAMBIGUOUS.**	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
4. The computer and network attack taxonomy meets the described characteristics of **REPEATABLE.**	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
5. The computer and network attack taxonomy meets the described characteristics of **ACCEPTED.**	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
6. The computer and network attack taxonomy meets the described characteristics of **USEFUL.**	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				

Proceed to the next page.

7. Please suggest any areas of improvement to the computer and network attack taxonomy that you observed.

Category	Area of Improvement
Attackers	
Tools	
Access	
Results	
Objectives	

Stop.

Please return the questionnaire to richard.daigle@afit.af.mil.

Thank you for your time and support.

Appendix B – 1997 Computer and Network Attack Questionnaire Summaries

This appendix contains the cumulative information obtained from the computer and network attack questionnaire. Table 12 lists all the respondents' comments, verbatim. Per the questionnaire's instructions, if the respondents selected Disagree or Strongly Disagree to questions 1 through 6, this researcher requested comments explaining their decision.

Table 13 lists all the respondents' suggested areas of improvements for the taxonomy,

verbatim.

Table 12 - 1997 Questionnaire Disagree and Strongly Disagree Comments

1. The computer and network attack taxonomy meets the described characteristics of **MUTUALLY EXCLUSIVE**.
- A hacker for example can do thing for more than one reason, i.e. for noteriety and financial gain.   - As explicitly defined, I can see clear distinctions between them (e.g. terrorist vs. corp. raider). However, nothing seems to preclude one attacker from "wearing 2 or more hats." For example, and using Mr. Howard's definitions, a terrorist may perform some "vandal"-ism (break in to computers to cause damage) for the express purpose of supporting his political objectives. Related would be a Corporate Raider who, in order to achieve financial gain (maybe win a lucrative contract) for his corporation, may hire a Professional Criminal to break into a competitor's system and cause damage (act as a "vandal") so as to improve the corporation's position relative to the competitor. It seems that either through employment of various tactics or enlistment of an intermediary an attacker can function on/across multiple "levels" and break the exclusivity of this taxonomy.   - For the "Attackers" category, there is (or can be) overlap between vandals and every other groups except for spies (they don't want you to know they were there). For example, a corporate raider can gain by damaging a competitors website -- would that be a corporate raider or a vandal? For the "Tools" category, there is overlap between several tools. For example, a toolkit (or distributed tool) is made up of autonomous agents and/or scripts or programs. There may also be overlap in the "Objectives" category akin to that in the "Attackers" category.
2. The computer and network attack taxonomy meets the described characteristics of **EXHAUSTIVE**.
- As described, this doesn't appear to account for attacks prosecuted as, or during, an act of war. Where do military operations (for whatever National Objective) fit in? Also as described, the ACCESS issue describes general points of system vulnerability; but fails to addess other means of "unauthorized use/access" (e.g. social engineering) that can defeat protected systems.   - Computers and Networks can be attacked by external means as well (microwave pulses, etc). Isn't that another tool terrorists could sue to impact comm networks.   - Social engineering should be part of the "Tools" category.   - Unsure how Denial of Service types of attacks would fit in the Access category. Also need a category for physical access.

| |
|---|
| 3. The computer and network attack taxonomy meets the described characteristics of **UNAMBIGUOUS**. |
| What if the financial gain of one company also causes damage? Under which one is it catagorized then? Different people may classify differently because of the "mutually exclusive" problems identified above. There might be existing toolkits that operate in a distributed fashion - so would it be classified as under the "toolkit" category, or the "distributed tool" category? |
| 4. The computer and network attack taxonomy meets the described characteristics of **REPEATABLE**. |
| What if the financial gain of one company also causes damage? Under which one is it catagorized then? Don't know if it's repeatable. I'm a comm officer and the taxonomy seems logical enough, but the common user may not come to the same conclusion. Perhaps this is a test within itself. Since there is a problem with ambiguity, there would also be a problem with repeatability. |
| 5. The computer and network attack taxonomy meets the described characteristics of **ACCEPTED**. |
| I don't agree with the term 'Accepted'. I believe it's acceptable, but using the word accepted within your argument may assert a precedent that will later call the study into question. Side note: I think you may gain some utility in breaking this questionnaire out to test each of the categories. |
| 6. The computer and network attack taxonomy meets the described characteristics of **USEFUL**. |
| No comments. |

Table 13 - 1997 Taxonomy Suggested Areas of Improvement

7. Please suggest any areas of improvement to the computer and network attack taxonomy that you observed.	
Category	**Area of Improvement**
Attackers	• Could also be "insiders", Users that accidentally cause damage to a system through ignorance, or "script kiddies" that are not quite hackers. • Needs to include the role of the warfighter. Again, the problem is of exclusivity since we (as a warfighter) may act to corrupt (e.g. for a deception), steal (e.g. critical technologies or codes), DOS (extend an adversay OODA loop and diminish positive control of its forces). • Another overlooked "attacker" is the activist--has political motivations like a Terrorist but without the fear factor. • Might want to include dummies. Computer security should also limit damage caused by authorized users making stupid decisions or taking stupid actions. • I'm not sure how to solve the problem with vandals overlapping with more than one group. Possibly break each group into benign and malignant types. For example, hackers and crackers. • Need to look at the Nation/State IW aspect. Also some consideration of inadvertent attacks by authorized insiders--a big problem in the Air Force.
Tools	• Could also add packet sniffer. • This is usually a multi-step process involving many tools. This model would seem to indicate choosing one or another. The real world doesn't work like that. • Social Engineering (SE) is a tool employed to gain unauthorized access. It is also a point of vulnerability...I'm unsure how/where to delineate SE. • Needs to acknowledge that sometimes (see "processes" comment within the Access category below) use of tools are not necessary. • Ensure people understand that attackers are not limited to the tools that line up with their respective blocks. All unauthorized personnel make use of the same tools to achieve their different objectives. • Not mutually exclusive. Toolkit seems to be an 'All of the above' category. • This category focused only on the technical aspects of computer and network attack. There are many instances where people give out user IDs and passwords to intruders so that no "tool" as defined in this taxonomy is required.

Category	Area of Improvement
7. Please suggest any areas of improvement to the computer and network attack taxonomy that you observed.	
Access	• Social Engineering is a significant point of vulnerability • As far as "processes" go, I think this is too limited. It refers to "protected" resources. What about when information is errantly or inadvertently "made available." It may be that an "attacker" doesn't even have to conduct an attack to get information, if that's what is desired.... • The access referred to here is unclear. Vulnerability seems to be how the attacker gets in, while unathorized access and use describes what the attacker is doing, and processes, files, and data in transit refer to what the attacker is after. The AF categorizes "Access" into root and user-level access. • I would expect this to address the fact that DoS attacks can be successful without ever gaining "access" to resources under control of the target.
Results	• Another possible result is Financial Loss, or loss of customer goodwill. • An attacker may "posturing" (e.g. creating backdoors, positioning tools, etc.) himself to take some later action without conducting one of the listed "results." • The view presented in the taxonomy is one of immediacy. It needs to consider the concept of investment as a potential desire or action of an attacker to achieve long-term gain. • Consider adding permanent destruction of information. I know it can fall under corruption, but I think there is a significant difference between manipulating data and destroying data. A manipulation can force a competitor's hand, whereas destruction can result in a closing or worse. • Theft of service and denial of service are very similar. By stealing bandwidth, even if you do not affect the users on line, other users may not be able to gain access. This is hard to ascertain.
Objectives	• Seems like there are more objectives than just these few. • Again, not mutaully exclusive in this area. • Distinction is made between personal and corporate financial gain in defining an attacker; why not make the distinction regarding the intended objective. • Including the warfighter as an attacker will impact this area. Politial gain could be adapted to include National Objectives, but it seems other changes would also be required. • For the Dummies category, the objective would most likely be authorized use. • Again, the comments from the "Attacker" category apply here. • May also consider attacks with no well thought-out motivation, objectives may be entertainment or education, even "none".

Appendix C - 1998 Computer and Network Taxonomy Questionnaire

This questionnaire supports the thesis, An Analysis of the Computer and Network Attack Taxonomy, written by Captain Richard C. Daigle, graduate student in the Information Resource Management degree program. Read the background information on Figure 1 – Computer and Network Attack Taxonomy and then proceed to the questionnaire. Your contributions will be used to analyze the **satisfactory** usefulness of the computer and network attack taxonomy, as defined by Mr. John D. Howard. Please return the questionnaire to richard.daigle@afit.af.mil.
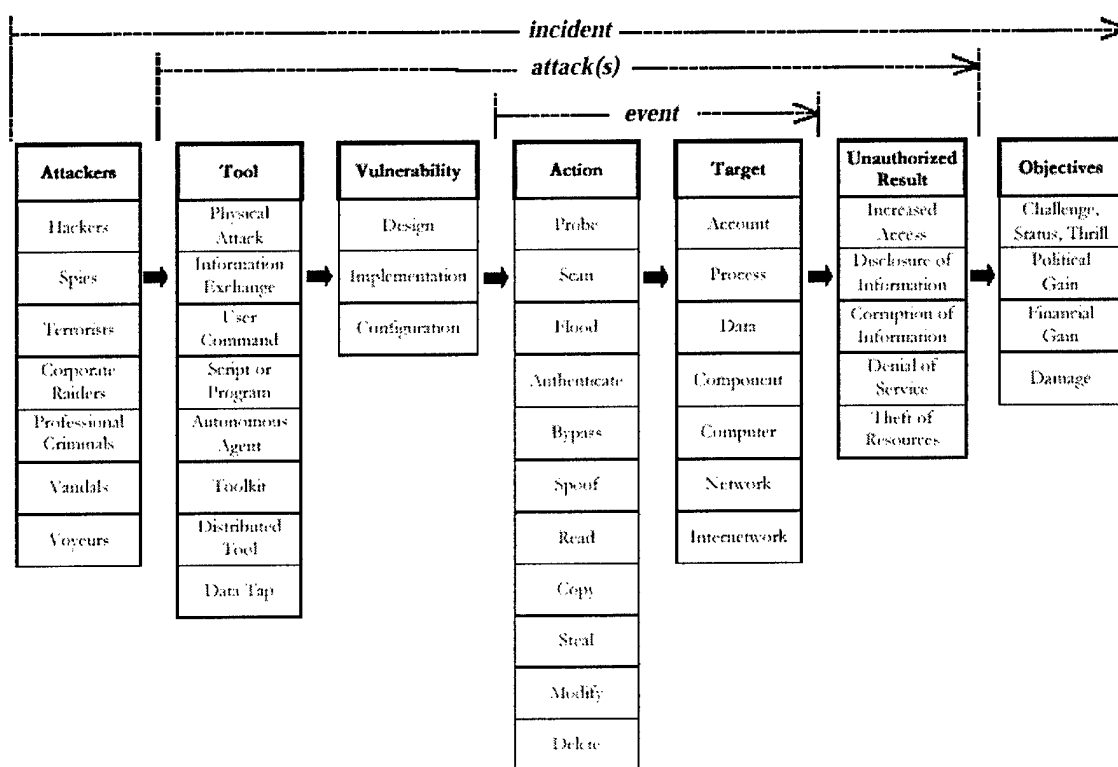
(Howard and Longstaff, 1998: 16)

Figure 1 – Computer and Network Attack Taxonomy

Howard developed this taxonomy as part of a collaborative effort with Security and Networking Research Group at the Sandia National Laboratories, Livermore CA, and the CERT Coordination Center at Carnegie Mellon University, Pittsburgh, PA. The taxonomy and resulting work was published in the 1998 Sandia National Laboratories

report, <u>A Command Language for Computer Security Incidents</u> by John D. Howard and

Thomas A. Longstaff, posted on the CERT®/CC web site at

http://www.cert.org/research/taxonomy_988667.pdf.

The following background information comes from a compilation of extracts from

Howard's research:

This taxonomy depicts a simplification of the path an attacker must take in order to accomplish the attacker's objectives. To be successful, an attacker must find one or more paths that can be connected, perhaps simultaneously.

Howard defined computer security as:

Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks. (50)

As the formal definition of computer security presented indicates computer security is preventing attackers from achieving objectives by making any complete connections through the steps depicted. More specifically, computer security efforts are aimed at the five blocks of the taxonomy.

A popular and simple taxonomy of computer and network security attacks is a list of single, defined terms. Variations of this approach include lists of categories. There are several problems that limit the usefulness of these approaches including 1) the terms not being mutually exclusive, 2) an exhaustive list being difficult to develop and unmanageably long, 3) the definitions of individual terms being difficult to agree on, and 4) there being no structure to the categories.

An alternate categorization method is to structure the categories into a matrix. The procedure for classification using these taxonomies, however, is not unambiguous when actual attacks are classified. In addition, the logic is not intuitive, and the classifications are limited in their usefulness.

The taxonomy developed as part of this research does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather to reorient the focus of the taxonomy toward a process, rather than a single classification category.

The final taxonomy presented was developed from the specific definition of computer security...from the criticisms of the current taxonomies, and from a process or operational viewpoint. From this viewpoint, an attacker on computers or networks attempts to link to ultimate objectives or motivations. This link is established through an operational sequence of tools, access, and results that connects these attackers to their objectives...

The taxonomy "does not attempt to enumerate all computer security flaws, or to enumerate all possible methods of attack, but rather attempts to provide a broad, inclusive framework. The intention was to reorient the focus of the taxonomy toward a process, rather than a single classification category, in order to provide both an adequate classification scheme for Internet attacks, and also a taxonomy that would aid in thinking about computer and network security".

Extracted from An Analysis of Security Incidents on the Internet 1989 – 1995, by John D. Howard, http://www.cert.org/research/JHThesis/Start.html.

The following information further helps you understand the computer and network attack

taxonomy:

Overarching Groupings

---

1. Incident - a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing.
2. Attack(s) - a series of steps taken by an attacker to achieve an unauthorized result.
3. Event - an action directed at a target which is intended to result in a change of state (status) of the target.

ATTACKERS

---

1. Attacker represents an individual who attempts one or more attacks in order to achieve an objective.

   a. Hackers - break into computers primarily for the challenge and status of obtaining access.
   b. Spies - break into computers primarily for information which can be used for political gain.
   c. Terrorists - break into computers primarily to cause fear which will aid in achieving political gain.
   d. Corporate Raiders - employees of one company break into computers of competitors for financial gain.
   e. Professional Criminals - break into computers for personal financial gain (not as a corporate raider).
   f. Vandals - break into computers primarily to cause damage.
   g. Voyeurs - attackers who attack computers for the thrill of obtaining sensitive information.

TOOLS

---

2. Tools used to exploit computer and network vulnerabilities.

a. Physical Attack - a means of physically stealing or damaging a computer, network, its components, or its supporting systems (such as air conditioning, electric power, etc.).
b. Information Exchange – a means of obtaining information either from other attackers (such as through an electronic bulletin board), or from the people being attacked (commonly called social engineering).
c. User Command - a means of exploiting a vulnerability by entering commands to a process through direct user input at the process interface.
d. Script or Program - a means of exploiting a vulnerability by entering commands to a process through the execution of a file of commands (script) or a program at the process interface.
e. Autonomous Agent - a means of exploiting a vulnerability by using a program, or program fragment, which operates independently from the user.
f. Toolkit - the attacker uses a software package which contains scripts, programs, or autonomous agents that exploit vulnerabilities.
g. Distributed Tool - a tool that can be distributed to multiple hosts, which can then be coordinated to anonymously perform an attack on the target host simultaneously after some time delay.
h. Data Tap - a means of monitoring the electromagnetic radiation emanating from a computer or network using an external device.

VULNERABILITY

3. A weakness in a system allowing unauthorized action

   a. Design - a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability.
   b. Implementation - a vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design.
   c. Configuration - a vulnerability resulting from an error in the configuration of a system, such as having system accounts with default passwords, having "world write" permission for new files, or having vulnerable services enabled.

ACTION

4. A weakness in a system allowing unauthorized action

   a. Probe – access a target in order to determine its characteristics.
   b. Scan – access a set of targets sequentially in order to identify which targets have a specific Characteristic.
   c. Flood – access a target repeatedly in order to overload the target's capacity.
   d. Authenticate – present an identity of someone to a process and, if required, verify that identity, in Order to access a target.
   e. Bypass – avoid a process by using an alternative method to access a target.
   f. Spoof – masquerade by assuming the appearance of a different entity in network communications.

g. Read – obtain the content of data in a storage device, or other data medium.
h. Copy – reproduce a target leaving the original target unchanged.
i. Steal – take possession of a target without leaving a copy in the original location.
j. Modify – change the content or characteristics of a target.
k. Delete – remove a target, or render it irretrievable.

TARGET

---

5. A computer or network logical entity (account, process, or data) or physical entity. (component, computer, network or internetwork).

a. Account – a domain of user access on a computer or network which is controlled according to a record of information which contains the user's account name, password and use restrictions.
b. Process – a program in execution, consisting of the executable program, the program's data and stack, its program counter, stack pointer and other registers, and all other information needed to execute the program.
c. Data – representations of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. Data can be in the form of files in a computer's volatile or non-volatile memory, or in a data storage device, or in the form of data in transit across a transmission medium.
d. Component – one of the parts that make up a computer or network.
e. Computer – a device that consists of one or more associated processing units and peripheral units, that is controlled by internally stored programs, and that can perform substantial computations, including numerous arithmetic operations, or logic operations, without human intervention during execution. Note: may be stand alone, or may consist of several interconnected units.
f. Network – an interconnected or interrelated group of host computers, switching elements, and interconnecting branches.
g. Internetwork – a network of networks.

UNAUTHORIZED RESULT

---

6. Unauthorized results are an unauthorized consequence of an event.

a. Increased Access - an unauthorized increase in the domain of access on a computer or network.
b. Disclosure of Information - the dissemination of information to anyone who is not authorized to access that information.
c. Corruption of Information – unauthorized alteration of data on a computer or network.
d. Denial of Service - the intentional degradation or blocking of computer or network resources.
e. Theft of Resources - the unauthorized use of computer or network resources.

7. The purpose or end goal of an incident.

   a. Challenge, Status, Thrill – objective of hackers and voyeurs
   b. Political Gain – objective of spies and terrorists
   c. Financial Gain – objective of corporate raiders and professional criminals
   d. Damage – objective of vandals

   According to Howard, a **satisfactory** taxonomy "should have classification

categories with the following characteristics" (53):

   a. Mutually exclusive - classifying in one category excludes all others because categories do not overlap
   b. Exhaustive - taken together, the categories include all possibilities
   c. Unambiguous - clear and precise so that classification is not uncertain, regardless of who is classifying
   d. Repeatable - repeated applications result in the same classification, regardless of who is classifying
   e. Accepted - logical and intuitive so that they could become generally approved
   f. Useful - can be used to gain insight into the field of inquiry. (53)

Therefore, based upon the five category descriptions and the **satisfactory** taxonomy

definition, please complete the following questionnaire to determine the degree that you

agree with the assessment that the computer and network attack taxonomy is

satisfactory. Since a taxonomy approximates reality, it may be limited in some of the

characteristics.

Please answer the questions and short answers below. If you select **Disagree** or **Strongly Disagree** for questions 1 through 6, please provide an explanation.

- Date: _____

- Primary Air Force Specialty or corresponding job description (i.e. Communications-Computer Officer): _____

Question	Strongly Agree	Agree	Disagree	Strongly Disagree
1. The computer and network attack taxonomy meets the described characteristics of **MUTUALLY EXCLUSIVE**.	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
2. The computer and network attack taxonomy meets the described characteristics of **EXHAUSTIVE**.	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
3. The computer and network attack taxonomy meets the described characteristics of **UNAMBIGUOUS**.	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
4. The computer and network attack taxonomy meets the described characteristics of **REPEATABLE**.	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
5. The computer and network attack taxonomy meets the described characteristics of **ACCEPTED**.	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				
6. The computer and network attack taxonomy meets the described characteristics of **USEFUL**.	☐	☐	☐	☐
If Disagree or Strongly Disagree selected, insert comments:				

Proceed to the next page.

7. Please suggest any areas of improvement to the computer and network attack taxonomy that you observed.

Category	Area of Improvement
Attackers	
Tools	
Vulnerability	
Action	
Target	
Unauthorized Result	
Objectives	

Stop.

Please return the questionnaire to richard.daigle@afit.af.mil.

Thank you for your time and support.

Appendix D – 1998 Computer and Network Attack Questionnaire Summaries

This appendix contains the cumulative information obtained from the 1998 computer and network attack questionnaire. Table 14 lists all the respondents' comments, verbatim. Per the questionnaire's instructions, if the respondents selected Disagree or Strongly Disagree to questions 1 through 6, this researcher requested comments explaining their decision. Table 14 lists all the respondents' suggested areas of improvements for the taxonomy, verbatim.

Table 14 - 1998 Questionnaire Disagree and Strongly Disagree Comments

1. The computer and network attack taxonomy meets the described characteristics of **MUTUALLY EXCLUSIVE**.
• Internal users "attack" networks more often than external attackers, sometimes they do it unknowingly sometimes with ulterior motives. I guess it depends on what your definition of an attack is. Perhaps your taxonomy should include such a definition. • Objectives are not neccesarily mutually exclusive. An atacker for example could be doing it for finacial gain and noteriety,
2. The computer and network attack taxonomy meets the described characteristics of **EXHAUSTIVE**.
• While overarching, nothing can possibly include ALL possibilities
3. The computer and network attack taxonomy meets the described characteristics of **UNAMBIGUOUS**.
• Some actions specifically can be classified differrently by different people, depending on their own interpretation
4. The computer and network attack taxonomy meets the described characteristics of **REPEATABLE**.
• See previous comments on differing interpretations
5. The computer and network attack taxonomy meets the described characteristics of **ACCEPTED**.
• No comments.
6. The computer and network attack taxonomy meets the described characteristics of **USEFUL**.
• No comments.

Table 15 - 1998 Taxonomy Suggested Areas of Improvement

7. Please suggest any areas of improvement to the computer and network attack taxonomy that you observed.	
Category	**Area of Improvement**
Attackers	• Much better than the last. I believe all bases are covered and they all make sense. • Good Coverage -- Skill level of the attacker would not be important to the process • Since there is a distinctin between hackers and crackers, it might warrant mentioning. • Note that there are fine lines for which an attacker can move into another name, for instance, voyeurs, if they do more than watch, might become one of the other classifications.
Tools	• I still see some overlap between toolkit and the Tools that make up the toolkit. • Data Tap can also include monitoring electrical usage of key components to determine complexity of access codes. Also known as Differential Power Analysis (Denning 1999) • "Process interface" - does this mean the computer directly? I'm assuming it means something more broad so that "computer" isn't a narrowing of scope.
Vulnerability	• Complete as is • Worth mentioning that "configuration" is attributable to the human factor. Specifically, a system can have superior design and implementation, but still be vulnerable because humans used incorrect configuration - the only as strong as the weakest link concept.
Action	• Good • No changes needed • As noted, differing interpretations can lead to different action classifications. Detailed explanations for each action area can alleviate this problem.
Target	• Good • No changes needed
Unauthorized Result	• Good • No changes needed
Objectives	• Good • No changes needed • These are not neccesarily mutually exclusive objectives.

Appendix E - AFCERT Base Incident Response Checklist

If you suspect or know a system is compromised, please follow these procedures and complete the form.

DON'T
- Finger attempt to access the source, or contact the source.
- Change the system files on the suspected/compromised system.
- Connect to the system over the network.

DO
- Unplug the machine from the network (if mission will allow).
- Log-on as root at the console and do a complete dump of the system (i.e., on Unix, **dd if="harddrive"of="tapedrive" bks=32k**). Make sure you don't alter any files on the system.
- Place the dump in a secure location.
- Place the suspected/compromised system in a secure place. (Limit access to the system).
- Complete the following and contact the AFCERT at DSN 969-3156 or 1-800-851-0187:

1. Report Originator Information:

    a. Name:
    b. Rank:
    c. Unit/Base:
    d. DSN Phone Number:
    e. Commercial Phone Number:
    f. Position (system administrator, security manager, etc.):
    g. MAJCOM:
    h. E-Mail Address:
    i. Message Address:
    j. Mailing Address:

2. Target Information (if additional targets use separate sheet):

    a. Network Domain Name (i.e., afcert.csap.af.mil):
    b. IP Address (i.e., 132.28.145.43):
    c. Computer Model (i.e., Sun SparcStation 10):
    d. Operating System/Version (SUN-OS 4.1.6 etc.):
    e. Security Mode of Operation (dedicated, system high, multilevel etc.):
    f. Security Classification (i.e., SBU, secret, etc.):
    g. Network/System Mission (i.e., administration, C2, communications, logistics, Domain Name Server, etc.):
    h. Network Structure/Type:
    i. How Detected:
    j. Impact on Mission (if compromised):
    k. AIS Auditing:

3. Attack Session Information (correlates with the target information):
(if known, include; if unknown, leave blank and don't access system files)

    a. Date/dates of the Session:
    b. Time:
    c. Attack Method:
    d. Success:
    e. Account (Include host name if available):
    f. First Layer Point of Origin IP:

4. Brief Scenario (Description of incident):

5. Countermeasure(s) Installed (e.g., patches, top wrappers, shadow passwords, etc.)

    a. Name and date installed (if known, include; if unknown, leave blank and don't access system files):

6. Notification Checklist (Indicate full name and rank, date, and time notified):

    a. Computer System Security Officer (CSSO):
    b. Operation Commander:
    c. Designated Approving Authority (DAA):
    d. Wing IP Office:
    e. MAJCOM IP Office:
    f. Air Force Computer Emergency Response Team:

(AFCERT, *Checklist*, 2000)

Appendix F - AFCERT Malicious Logic Report Format

1. Reporting period:

2. Reporting Information:

    a. Name/Rank:
    b. Unit:
    c. Base:
    d. MAJCOM:

3. Malicious logic name (complete section 3a-e for each malicious logic detect d):

    a. Number of infections detected by system mission criticality and point of detection:

TYPE SYSTEM* After	# Detected Before Infection	# Detected Infection
Mission Critical	_____	
Mission Essential	_____	
Mission Impaired	_____	
Non-Mission Essential	_____	

    *Criticality IAW AFMAN 10-401

    b. Number of work hours expended:

    c. Operating system and version:

    d. List standard system(s) affected (if applicable, i.e., GCCS, CAMS, FAMS):

    e. Source of infection, if known:

        ___ AF software
        ___ COTS or outside source
        ___ Personal disks
        ___ Downloaded files

                (AFCERT, *Report*, 2000; AFSSI 5021, 1996:15)

Appendix G - ACERT Intrusion Submission Form

Intrusion Response Checklist

If you suspect or know a system is compromised, please follow these procedures and complete the form.

DON'T

Finger attempt to access the source, or contact the source.

Change the system files on the suspected/compromised system.

Connect to the system over the network.

DO

Unplug the machine from the network (if mission will allow).

Log-on as root at the console and do a complete dump of the system

Make sure you don't alter any files on the system.

Place the dump in a secure location.

Place the suspected/compromised system in a secure place. (Limit access to the system).

Complete the following and contact the ACERT at DSN 235-1113 or 1-703-706-1113:

Email the ACERT at: acert@liwa.belvoir.army.mil

Or contact RCERT CONUS at DSN 879-2482 or (520) 538-2482:

Email the RCERT at: rcert-conus@rcertc.army.mil

1. **Report Originator Information**: Date: _____

a. Name _____ b. Rank/Grade _____

c. Unit/Post _____ d. DSN Phone Number _____

e. Commercial Phone Number _____

f. Position (system administrator, security manager, etc.)
_____

g. MACOM _____ h. e-mail Address _____

i. Message Address _____

j. Mailing Address _____

2. Target Information (if additional targets use separate sheet):

a. Network Domain & Host Name (i.e., liwa.belvoir.army.mil)
_____

b. IP Address (i.e., 132.28.145.43) _____Subnet
Mask_____

c. Computer Model (i.e., Sun SPARCstation
10)_____

d. Operating System/Version (SUN-OS 4.1.6 etc.)
_____

e. Security Mode of Operation (dedicated, system high, multilevel etc.)
_____

f. Security Classification (i.e., SBU, secret, etc.)
_____

g. Network/System Mission (i.e., administration, C2, communications, logistics, Domain
Name Server, etc.) _____

h. Network Structure/Type _____

i. How
Detected_____

j. Impact on Mission (if compromised)
_____

k. AIS
Auditing_____Yes_____No_____Type_____

l. Firewall _____Yes
____No_____Type_____

m. IDS _____Yes
_____No_____Type_____

n. System Status _____On-line _____Off-line

3. Attack Session Information (correlates with the target information):

(if known, include; if unknown, leave blank and don't access system files)

a. Date/dates and time of the Session Start: _____ Stop _____

b. Attack Method_____

c. Source IP_____

d. Source Host & Netblock name if available) Host _____Netblock_____

e. Organization: (i.e.. fl3m, TheK)_____

f. Country:

_____

4. Countermeasure(s) Installed (e.g., patches, TCP wrappers, shadow passwords, etc.)

a. Name and date installed:

_____

(if known, include; if unknown, leave blank and don't access system files)

5. Brief Scenario (Description of incident)

<div align="right">(ACERT, Intrusion, 2001)</div>

Appendix H - ACERT Virus Reporting Form

1. PERSON REPORTING INFORMATION:

    Name: _____ Title (ISSO/IAM/etc):
_____

    Phone: DSN _____ or Commercial
_____

    E-mail:
_____

    —

    Agency, Location, and MACOM:
_____

2. ANTI-VIRUS SOFTWARE PRODUCT INFORMATION (AT THE TIME OF INFECTION):

    AV Product Used (Norton/McAfee):
_____

    AV Product Version and Build #:
_____

    Scan Engine:
_____

    Virus Definition Date:
_____

3. VIRUS INFORMATION:

    Name of Virus:
_____

    Name of Infected File(s):
_____

    Date Detected: _____ Date Cleaned:
_____

    Detected at (Firewall, Exchange Server, Gateway, Desktop, etc.):
_____

4. COMPUTER INFORMATION:

    Operating System with Version and SP #s:
_____

    Additional Software with Ver/SP #s (Exchange Server, etc.):
_____

    IP Address of Infected System(s):
_____

5. DAMAGE REPORT:

Source of Infection (Check as Applicable):

___ E-mail (Originator's E-mail Address -
_____)

___ Download (URL -
_____)

___ Other
(_____)

Total # of Files Infected:
_____

Total # of Computers Infected:
_____

Type of Network (NIPRNET, SIPRNET, etc.):
_____

Impact of Virus on Mission:

___Total Loss ___Partial Loss ___Recovered Fully

Lost Manhours: _____

6. SYNOPSIS (Provide a description of the incident, to include identification of root cause(s) of infection and corrective steps taken):

Submit to the ACERT (virus@liwa.belvoir.army.mil) with a "cc" to your supporting RCERT.

(ACERT, *Virus*, 2001)

Appendix I - CERT®/CC Incident Reporting Form

Your contact and organizational information

1. Name...:
2. Organization name...:
3. Sector type (such as banking, education, energy or public safety)...:
4. Email address...:
5. Telephone number...:
6. Other...:

Affected Machine(s)
(duplicate for each host)

7. Hostname and IP...:
8. Timezone...:
9. Purpose or function of the host (please be as specific as possible)...:

Source(s) of the Attack
(duplicate for each host)

10. Hostname or IP...:
11. Timezone...:
12. Been in contact?...:
13. Estimated cost of handling incident (if known)...:
14. Description of the incident (include dates, methods of Intrusion, intruder tools involved, software versions and patch levels, intruder tool output, details of vulnerabilities exploited, source of attack, or any other relevant information)...:

(CERT®/CC, *Form*, 2000)

Appendix J - DOD CERT Incident Reporting Form

DOD CERTDOD CERT

Incident Reporting Form

This form meets the initial reporting requirements outlined in CJCSI 6510.01B, Change 1, to report computer/network events. Please use the virus reporting form on the DOD CERT home page to submit detailed virus reports. Keep in mind that the security classification of your incident is dependent on the classification of the system affected. If you are unable to email this form, you may send it by FAX to 703-607-4009 (DSN: 327-4009).

Report Classification (e.g., For Official Use Only)
Warning: This is an UNCLASSIFIED system. Enter Only Unclassified Information.
Use SIPRNet to report classified incidents.

From:__
To:__
Date/Time of Report:__   (Date & Time(ZULU) of Report (e.g. dd/mm/yyyy/hhmmZ))
Type of Incident:__   (Probe Scan DNS Denial of Service User level Access Root Level

Access Malicious Logic)
Name of Asset:__   Machine Name
Mission Impact:__

Details of Incident: (See Reporting Guidelines for more detail information.)

Who:__   IP Address of Source (e.g. xxx.xxx.xxx.xxx)
What:__   Web Server DNS Server File Server Mail Server Multi-Function Server
     Router Firewall Workstation Machine Function
When:__   Date & Time(ZULU) of Incident (e.g. dd/mm/yyyy/hhmmZ)
Where: __   IP Address of Destination (e.g. xxx.xxx.xxx.xxx)
Why:__
Action Taken:__
Contact Information:__
Coordination:__

Reporting Classification (e.g. For Official Use Only)
Warning Reminder: This is an UNCLASSIFIED system.
Enter Only Unclassified Information.

(Department of Defense, 2001)

Appendix K - FeDCIRC Reporting Form

version 4.3.6
October 1999

Federal Computer Incident Response Capability
(FedCIRC)
Incident Reporting Form

FedCIRC has developed the following form in an effort to gather incident information. If you believe you are involved in an incident, we would appreciate your completing the form below. If you do not believe you are involved in an incident, but have a question, send email to:

    fedcirc@fedcirc.gov

Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Return this form to:

    fedcirc@fedcirc.gov

If you are unable to email this form, please send it by FAX. The FedCIRC FAX number is:

    +1 412 268 6989

Your contact information
name ....:
email address...:
telephone number:
other...........:

Affected Machine(s)
(duplicate for each host)
hostname and IP.:
timezone........:

Source(s) of the Attack
(duplicate for each host)
hostname or IP..:
timezone........:
been in contact?:

Description of the incident

(Include dates, methods of intrusion, intruder tools involved, software versions and patch levels, intruder tool output, details of vulnerabilities exploited, source of attack, or any other relevant information.)

(FedCirc, 2001)

Appendix L - NAVCIRT Incident Reporting Form

1. Incident date
2. Physical location of the system attacked
3. How was the attack identified
4. How access was obtained
5. Vulnerability exploited
6. Actions attempted during session
7. Highest classification of information involved
8. Evaluation of attack success
9. Damage or effects resulting from attack
10. Hardware Configuration
11. Operating System
12. Security Software installed
13. Origination point of incident
14. Indication of additional activity
15. IP address
16. Names used
17. Mission of system attacked (e.g. administration, command and control, message handling, etc.)
18. Point of contact (e.g. name, phone number, e-mail address)
19. Additional information

Viruses: Those known viruses with countermeasures available in the NAVCIRT tool–kit should be logged and reported to FLTINFOWARCEN on a monthly basis. Only those viruses not known or without an available countermeasure will be reported […].

(Department of the Navy, 1998)

Appendix M - Recommended Standard Information Collection Form

PAGE 1 OF 2
ORIGINATOR INFORMATION

1. DATE OF REPORT:
2. TIME (ZULU/GMT):
3. REPORTERS NAME:
4. ORGANIZATION NAME:
5. LOCATION COUNTRY:
6. LOCATION CITY:
7. LOCATION STATE/PROVINCE:
8. POSTAL MAILING ADDRESS:
9. PHONE:
10. EMAIL:
11. WEBSITE:
12. ADDITION INFORMATION YOU DEEM IMPORTANT:

AFFECTED SYSTEM(S) INFORMATION

13. DATE OF ATTACK:
14. TIME (ZULU/GMT):
15. HOST NAME (LIST ALL):
16. NETWORK DOMAIN NAME (TOP.MID.DNS):
17. IP ADDRESS (XXX.XX.XXX):
18. COMPUTER MODEL NAMES:
19. OPERATING SYSTEM/VERSION:
20. SECURITY MODE OF OPERATION:
21. SECURITY CLASSIFICATION:
22. ADDITIONAL INFORMATION YOU DEEM IMPORTANT:

ATTACK/INCIDENT INFORMATION

COMPLETE TO THE BEST OF YOUR ABILITY.
THE MORE INFOMRATION, THE BETTER.
PLEASE EXPLAIN "OTHER" SELECTION FULLY.

1 ATTACKER	SELECT ALL THAT APPLY
CORPORATE RAIDER	
HACKER	
PROFESSIONAL CRIMINAL	
SPIES	
TERRORIST	
VANDALS	
VOYEURS	
OTHER	

5 TARGET	SELECT ALL THAT APPLY
ACCOUNT	
COMPONENT	
COMPUTER	
DATA	
INTERNETWORK	
NETWORK	
PROCESS	
OTHER	

2 TOOL	SELECT ALL THAT APPLY
AUTONOMOUS AGENT	
DATA TAP	
DISTRIBUTED TOOL	
INFORMATION EXCHANGE	
PHYSICAL ATTACK	
SCRIPT OR PROGRAM	
TOOLKIT	
USER COMMAND	
OTHER	

6 UNAUTHORIZED RESULT	SELECT ALL THAT APPLY
CORRUPTION OF INFORMATION	
DENIAL OF SERVICE	
DISCLOSURE OF INFORMATION	
INCREASED ACCESS	
THEFT OF SERVICE	
OTHER	

3 VULNERABILITY	SELECT ALL THAT APPLY
CONFIGURATION	
DESIGN	
IMPLEMENTATION	
OTHER	

7 OBJECTIVES	SELECT ALL THAT APPLY
CHALLENGE, STATUS, THRILL	
DAMAGE	
FINANCIAL GAIN	
POLITICAL GAIN	
OTHER	

4 ACTION	SELECT ALL THAT APPLY
AUTHENTICATE	
BYPASS	
COPY	
DELETE	
FLOOD	
MODIFY	
PROBE	
READ	
SCAN	
SPOOF	
STEAL	
OTHER	

104

Works Cited

Abbate, Janet. Inventing the Internet. Cambridge, Massachusetts: MIT Press, 1999.

Abreu, Elinor. "Teen arrested for Web attack on CNN.com," 21 Apr 2000. Federal Computer Week. http://www.fcw.com/fcw/articles/2000/0417/web-teen-04-21-00.asp. 29 Jul 2000.

"Acceptable." Def. 1. The American Heritage Dictionary. 3rd ed. 1996.

"Accepted." Def. 1. The American Heritage Dictionary. 3rd ed. 1996.

ACERT U.S. Army Computer Emergency Response Team. Intrusion Response Checklist. https://www.acert.belvoir.army.mil/forms/checklist.htm. 2 Mar 2001.

-----. ACERT Virus Reporting Form. https://www.acert.belvoir.army.mil/virusinfo/acertvrpf.htm. 2 Mar 2001.

Air Force Computer Emergency Response Team [AFCERT]. Welcome to the AFCERT. http://afcert.csap.af.mil. 26 Sep 2000.

-----. Base Incident Response Checklist. http://www.afcert.kelly.af.mil/ir_checklist.html. 10 Nov 2000.

-----. Malicious Logic Report Format. http://www.afcert.kelly.af.mil/virus_report.txt. 10 Nov 2000.

Air Force News [AFN]. "AFRL Information Directorate will manage major portion of NGI research," 15 Jun 1998. http://www.af.mil/news/Jun1998/n19980615_980841.html. 29 Jul 2000.

-----. "DOD on alert against computer intrusions," 26 Feb 1998. http://www.af.mil/news/Feb1998/n19980226_980245.html. 29 Jul 2000.

-----. "Hacker leaves mark on Web site," 3 Mar 1999. http://www.af.mil/news/Mar1999/n19990303_990335.html. 29 Jul 2000.

-----. "Hacker targets Air Force home page," 31 Dec 1996. http://www.af.mil/news/Dec1996/n19961231_961333.html. 29 Jul 2000.

-----. "Theft, crime rise on net, bugs users," 10 Sep 1999. http://www.af.mil/news/Sep1999/n19990910_991681.html. 29 Jul 2000.

Bartlett, John. Familiar Quotations: A Collection of Passages, Phrases, and Proverbs Traced to Their Sources in Ancient and Modern Literature. ed. Emily Morison Beck. Boston: Little, Brown and Co. 1980.

Brewin, Bob. "Kosovo ushered in cyberwar," Federal Computer Week, 27 Sep 1999: 1+.

Briney, Andy. "Security Focused," Information Security, September 2000: 40-68.

CERT® Coordination Center [CERT®/CC]. An Analysis Of Security Incidents On The Internet 1989 – 1995. http://www.cert.org/research/JHThesis/Start.html. 1 Mar 2001.

-----. DARPA Establishes Computer Emergency Response Team. 31 Dec 1988. http://www.cert.org/about/1988press-rel.html. 3 Mar 2001.

-----. Incident Reporting Form. Version 5.2. April 2000. http://www.cert.org/reporting/incident_form.txt. 8 Nov 2000.

Department of Defense Computer Emergency Response Team. Incident Reporting Form. Version 5.2. April 2000. ftp://www.cert.mil/pub/info/general/network.security/report.html. 5 Mar 2001.

-----. Meet the CERT® Coordination Center. 5 Sep 2000. http://www.cert.org/meet_cert/meetcertcc.html. 24 Oct 2000.

Department of the Air Force. Air Force Directory 33-303 [AFDIR 33-303] Compendium of Communications and Information Terminology. AFDIR 33-303. Washington: HQ USAF, 1 November 1999.

-----. Air Force Doctrine Document 2-5 [AFDD 2-5] Information Operations. AFDD 2-5. Washington: HQ USAF, 5 August 1998.

-----. Air Force Instruction 33-129 Transmission of Information via the Internet. AFI 33-129. Washington: HQ USAF, 1 August 1999.

-----. Air Force Systems Security Instruction 5021 Vulnerability and Incident Reporting [AFSSI 5021]. AFSSI 5021. Washington: HQ USAF, 16 August 1999.

-----. Global Engagement: A Vision for the 21st Century Air Force flows from the National Security. Washington: HQ USAF, 1996.

Department of the Navy. Navy and Marine Corps Computer Network Incident Response. OPNAV INSTRUCTION 2201.2. Washington: CNO and HQ USMC, 3 Mar 1988.

Deutch, John M. Director of Central Intelligence Agency. "Foreign Information Warfare Programs and Capabilities". Statement before US Senate Committee on Governmental Affairs; Permanent Subcommittee on Investigations. 25 June 1996.

Dooley, David. Social Research Methods. New Jersey: Prentice Hall, 1995.

Federal Computer Incident Response Center [FedCIRC]. Report An Incident. http://www.fedcirc.gov/. 2 Mar 2001.

Fogleman, Ronald R. Chief of Staff, United States Air Force. "The Fifth Dimension of Warfare". Speech to Armed Forces Communications and Electronics Association. Washington, D.C. 25 April 1995.

Government Accounting Office [GAO]. Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data. Report no. T-AIMD-99-146. Washington: GPO, 15 Apr 1999.

-----. Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements. Report no. T-AIMD-00-171. Washington: GPO, 10 May 2000.

-----. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Report no. T-AIMD-96-92. Washington: GPO, 22 May 1996.

-----. Information Security: Computer Attacks at Department of Defense Pose Increasing Risk. Report no. T-AIMD-96-84. Washington: GPO, 22 May 1996.

-----. Information Security: Computer Hacker Information Available on the Internet. Report no. T-AIMD-96-108. Washington: GPO, 5 Jun 1996.

-----. Information Security: Recent Attacks on Federal Web Sites Underscore Need for Stronger Information Security Management. Report no. T-AIMD-99-223. Washington: GPO, 24 Jun 1999.

-----. Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk. Report no. AIMD-98-22. Washington: GPO, 24 Jun 1999.

Hammer, Michael and James Champy. Reengineering the Corporation: A Manifesto for Business Revolution. New York: HarperCollins. 1993.

Hoffer, Jeffery A., Joey F. George, and Joseph S. Valacich. Modern Systems Analysis and Design. 2nd ed. Reading, MA: Addison-Wesley. 1998.

Howard, John D. An Analysis of Security Incidents on the Internet 1989 – 1995. Ph.D. dissertation. http://www.cert.org/research/JHThesis/Start.html. Carnegie Mellon University, Pittsburgh, PA. 7 April 1997.

-----. Interview. 3 Nov 2000.

Howard, John D., and Thomas A. Longstaff. A Common Language for Computer Security Incidents. Sandia Report. Albuquerque, NM: Sandia National Laboratories, October 1998 (SAND98-8667).

Huang, J. H. Sun Tzu: The Art of War, the New Translation. New York: William Morrow, 1993.

Internet Software Consortium [ISC]. Internet Domain Survey: July 2000. http://www.isc.org/ds/WWW-200007/index.html, 11 Nov 2000.

"Interpretation." Def. 1. The American Heritage Dictionary. 3rd ed. 1996.

Joint Chiefs of Staff [JCS]. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington: GPO, 9 Oct 1998.

Krippendorff, Klaus. Content Analysis : An Introduction To Its Methodology. Beverly Hills: Sage Publications. 1980.

McClave, James T., P. George Benson, and Terry Sincich. Statistics for Business and Economics. 7th ed. New Jersey: Prentice Hall, 1998.

Moschovitis, Christos J.P. et al. History of the Internet: A Chronology, 1843 to the Present. Santa Barbara, California: ABC-CLIO, 1999.

National Science Board [NSB]. Science & Engineering Indicators – 2000. (NSB-00-1)Arlington, VA: National Science Foundation. http://www.nsf.gov/sbe/srs/seind00/start.htm. 2000.

NSF Creation and Mission. 27 May 1999. http://www.nsf.gov/home/about/creation.htm. 19 July 2000.

OECD Online. Organisation for Economic Co-operation and Development. About OECD. 16 June 2000. http://www.oecd.org/about/. 16 June 2000.

Quoteland.com. 2000. http://www.quoteland.com/.

Roberts, Wess. Leadership Secrets of Attila the Hun. New York: Warner Books, Inc., 1985.

Rosengren, Karl Erik. ed. Advances In Content Analysis. Beverly Hills: Sage Publications. 1981.

Sakurai, Norihisa, Evangelos Ioannidis, and George Papaconstantinou. The Impact of R&D and Technology Diffusion on Productivity Growth: Evidence for 10 OECD Countries in the 1970s and 1980s. OCDC/GD(9)27. Paris, France: Head of Publications Service, OECD, 1996.

Schneider, Fred B., ed., et al. Trust in Cyberspace. Washington: National Academy Press. 1999.

"Taxonomy." Def. 3. The American Heritage Dictionary. 3rd ed. 1996.

United States Senate Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information. Crime, Terror, & War: National Security & Public Safety in the Information Age. 105th Congress, 1998. Washington: GPO, November 1998.

Verton, Daniel. "Feds schooled by 'zombies'," <u>Federal Computer Week</u>, 21 Feb 2000: 10.

-----. "Intercepts," <u>Federal Computer Week</u>, 1 May 2000: 50.

White, Richard and Greg Kincaid. "Information Warfare: An Overview of AFIWC Operations, version 2.3." Slide 20. Briefing at the USAF Academy, CO. February, 1996.

<u>World Development Indicators [WDI] 1999</u>. Sec. 5.11 The information age. The World Bank. 26 April 1999.

<u>Vita</u>

Captain Richard C. Daigle was born on ███████████ in Lafayette, Louisiana. He graduated from Acadiana High School in Lafayette in June 1981 and entered undergraduate studies at the University of Southwestern Louisiana in 1981. He enlisted in the US Air Force 1983 and spent 9 years as enlisted Continuous Photoprocessing Specialist and Computer Systems Programmer.

While assigned to the 1973 Communications Group, Maxwell AFB, Alabama, as a computer systems programmer, Richard re-enrolled in undergraduate studies at Troy State University at Montgomery and earned a Bachelor of Science degree in Computer Information Science in 1991. Upon graduation, the Air Force accepted Richard into the Officer Training Group in February 1993 and he received his commission in June 1993.

His first permanent assignment as a Communication-Computer Systems officer was to the NORAD System Support Facility, Tyndall AFB, as a computer programmer and computer systems instructor. He maintained the NORAD Air Operation Center software and personally developed several computer-training seminars.

He next accepted an assignment as a Command, Control, Communications, Computers, and Intelligence Staff Officer and Test Director in the Joint Interoperability Test Command at Fort Huachuca, Arizona, a field organization of DISA. Richard managed a 20-person team that conducted the installation and acceptance testing of the Defense Information System Network , he directed the development of the DOD Public Key Infrastructure testbed, and prepared the first Air Force site, Whiteman AFB, OH, for the initial site testing of the Defense Travel System.

He entered AFIT's Graduate Information Resource Management program at Wright-Patterson AFB, OH in September 1999 and graduated in March 2001.

1. REPORT DATE (DD-MM-YYYY) 20-03-2001	2. REPORT TYPE Master's Thesis	3. DATES COVERED (From – To) August 1999 – March 2001

4. TITLE AND SUBTITLE

AN ANALYSIS OF THE COMPUTER AND NETWORK ATTACK TAXONOMY

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Richard C. Daigle, Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/01M-04

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Information Warfare Center
Information Operations Technology Division (AFIWC/IOT)
Attn: Captain Shawna R. Wimpy
250 Hall Blvd, Ste 138
San Antonio, TX 78243   DSN 969-3990 ext 2069

10. SPONSOR/MONITOR'S ACRONYM(S)

AFIWC/IOT

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

Dr. Alan R. Heminger, ENV, DSN: 785-3636, ext. 4797

14. ABSTRACT

The Air Force's dependence on the Internet continues to increase daily. However, this increased dependence comes with risks. The popularity and potential of the Internet attracts users with illegal as well as legal intentions. Since the Air Force considers the Internet an integral component of its Information Operations strategy, the Air Force must be confident that it can trust the security of this component. Therefore, reliable methods and information that helps the Air Force classify the risks associated with the Internet can help the Air Force determine the best processes to assure the security of its use of this resource.

This thesis examines the computer and network attack taxonomy developed by John Howard. The taxonomy is a possible method that the Air Force can use to help it classify Internet security attacks and incidents.

This researcher concluded that the computer and network attack taxonomies were satisfactory. The questionnaire respondents appeared to prefer the 1998 version more. This researcher also concluded that organizations responsible for the collection and distribution of Internet security information, do explicitly collect some, not all, information useful as input into the taxonomy.

15. SUBJECT TERMS

Internet, Internet Security, Information Security, Information Assurance, Computer Security, Network Security, Intrusion Detection, Intruder Techniques, Intruder Methods, Vulnerabilities, Cybercrime, Information Operations, Information Warfare, Information Superiority, Computer Emergency Response Team (CERT).

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Dr. Alan Heminger, ENV
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code)
U	U	U	UU	121	(937) 255-3636, ext 4797

	Form Approved OMB No. 074-0188